VEILLE TECHNOLOGIQUE · BTS SIO SLAM · THÈME : CRYPTOGRAPHIE & SÉCURITÉ

Le Chiffrement Homomorphe — FHE & Zama

Protection des données · Cloud · Cryptographie avancée · CNIL, IBM France, Zama

CANIAUX Romain · 06 Mars 2026

Dans le cadre de mon BTS SIO SLAM, je mène une veille sur le thème de la **Cryptographie & Sécurité informatique**, un domaine directement lié à mon projet professionnel : développer des applications sécurisées dans des secteurs comme la santé, la finance ou l'administration publique. C'est en explorant ce thème que j'ai découvert le **chiffrement homomorphe (FHE)** et son industrialisation par des acteurs français comme Zama — une technologie qui répond à un problème concret : comment traiter des données sensibles dans le cloud sans jamais les exposer ?

1. PRÉSENTATION DU SUJET

Pourquoi ce sujet ? En effectuant ma veille sur la cryptographie et la sécurité des données, j'ai découvert le chiffrement homomorphe (FHE), une technologie présentée par la CNIL comme une évolution majeure de la protection des données. Ce qui m'a intéressé, c'est qu'elle répond à un problème concret en développement : comment traiter des données sensibles dans le cloud sans jamais les exposer ?

Ce qu'est le FHE : Selon la CNIL, le chiffrement homomorphe est une technique cryptographique permettant de réaliser des opérations sur des données chiffrées sans que celles-ci aient à être déchiffrées. Le résultat reste sous forme chiffrée et ne peut être lu que par le destinataire autorisé. Contrairement au chiffrement classique, les données ne sont donc jamais exposées, même lors de leur traitement.

2. RÉSUMÉ DES ARTICLES

FrenchWeb — Zama (juillet 2025) : Zama, startup française fondée par Rand Hindi et Pascal Paillier, a levé 57 millions d'euros en série B pour accélérer le déploiement de ses solutions FHE. Son moteur est désormais 100 fois plus rapide qu'à son lancement et traite plusieurs centaines de transactions par seconde grâce aux GPU. Plus de 5 000 développeurs utilisent déjà ses bibliothèques open source.

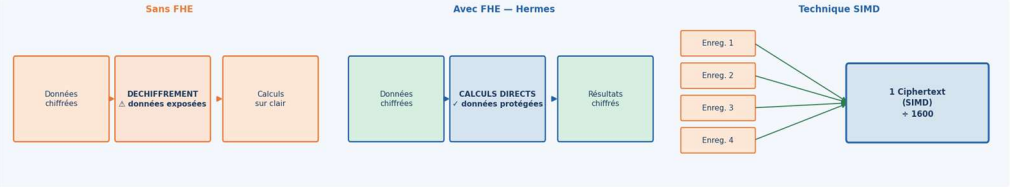

Figure 1 — Principe du FHE : calculs directs sur données chiffrées, sans déchiffrement

AWS France / Zama (septembre 2025) : Le témoignage client publié par Amazon Web Services France explique comment Zama s'appuie sur les instances AWS haute performance pour faire tourner ses algorithmes FHE. Le FHE permet d'entraîner ou d'exécuter des prédictions de modèles de Machine Learning sur des données confidentielles sans jamais les exposer — un cas d'usage concret pour les secteurs santé et finance.

Journal du Coin (décembre 2025) : Zama a lancé son mainnet fin décembre 2025 sur Ethereum, réalisant le premier transfert confidentiel de stablecoin grâce au FHE. L'article détaille comment la technologie permet aux développeurs de créer des applications manipulant des données sensibles sans jamais les exposer, en utilisant des bibliothèques open source compatibles Solidity.

3. CE QUE CETTE TECHNOLOGIE APPORTE ET SES LIMITES

Apports :

- Confidentialité totale côté serveur
- Adapté : santé, finance, défense
- Compatible SQL et vectoriel

Limites :

- Coût computationnel encore élevé
- Nécessite GPU/FPGA pour grande échelle

4. CAS D'USAGE CONCRETS

D'après les articles consultés, le FHE trouve des applications directes dans plusieurs secteurs soumis à de fortes contraintes réglementaires (RGPD) :

Figure 2 — Trois secteurs prioritaires identifiés par FrenchWeb, AWS France et Journal du Coin

- Santé : analyse de données médicales chiffrées sans exposer les informations patients, même au prestataire cloud.
- Finance : scoring bancaire et détection de fraude sur données clients chiffrées, garantissant la conformité RGPD — cas documenté par AWS France.
- Cloud : délégation de calculs à un serveur externe sans confier les données en clair — cas d'usage central selon Zama et Journal du Coin.

5. MON ANALYSE PERSONNELLE

Cette veille m'a permis de découvrir une technologie que je ne connaissais pas : le FHE. Ce qui m'a le plus marqué, c'est l'existence de Zama, une startup française qui rend le FHE accessible aux développeurs via des bibliothèques open source utilisées par plus de 5 000 développeurs dans le monde. En tant que futur développeur SLAM, je vois un intérêt direct : pouvoir concevoir des applications manipulant des données sensibles sans jamais les exposer côté serveur. Les limites actuelles (temps de calcul élevé) reculent rapidement — Zama affiche ×100 de gain de performance depuis son lancement, et AWS héberge déjà ses solutions en production.

CONCLUSION

Le chiffrement homomorphe sort progressivement des laboratoires de recherche pour devenir une technologie industrielle, portée en France par des acteurs comme Zama et des institutions comme la CNIL. Dans un contexte où le RGPD impose une protection renforcée des données personnelles, le FHE représente une piste concrète pour les développeurs qui souhaitent construire des applications respectueuses de la vie privée dès leur conception.

6. SOURCES CONSULTÉES (FORMAT APA)

Source	Titre de l'article	Année	Lien
CNIL	*Chiffrement homomorphe — Définition officielle*	*2024*	*www.cnil.fr/fr/definition/chiffrement-homomorphe*
FrenchWeb — Zama	*Zama lève 57M€ pour faire du FHE le socle de la finance on-chain*	*Juil. 2025*	*www.frenchweb.fr/zama-leve-57-millions-deuros-pour-faire-du-chiffrement-homomorphe-le-socle-de-la-finance-on-chain/455765*
AWS France — Zama	*Témoignage client Zama : FHE sur instances AWS haute performance*	*Sept. 2025*	Témoignage client : Zama
Journal du Coin — Zama	*Zama innove pour la distribution de ses tokens — mainnet FHE lancé*	*Déc. 2025*	*Zama : La licorne du FHE s'offre un Turbo ZK pour dominer la confidentialité On-Chain - Journal du Coin*