Quelles technologies pour assurer la confiance numérique ?

Anonymat, confidentialité, traçabilité souveraine

Vendredi 7 juin 2024

Coordination scientifique :

Christophe CALVIN (CEA)
David MENGA (Edf R&D)

Renseignements, programme… :

À la croisée des révolutions numériques

Table des matières

Compte-rendu du séminaire : Quelles technologies pour assurer la confiance numérique ?

Amphithéâtre Becquerel, école Polytechnique

1/ Introduction

Pour des raisons techniques et indépendances de la volonté des organisateurs, plusieurs intervenants sont absents, et de nombreuses vidéos ne sont pas disponibles.

Un mot d'introduction et de bienvenu est prononcé par David Menga. Selon lui, nous allons faire, ou faisons déjà face à une crise de confiance de la part du grand public dans le numérique. Et il faut travailler pour la rétablir ou l'améliorer. Tout le monde parle d'intelligence artificielle, de monnaie numérique, d'utilisation de la blockchain… Mais on oublie « joyeusement » les questions de respect de la vie privée, de confidentialité. Et c'est d'autant plus embêtant que ces technologies absorbent énormément d'informations personnelles pour être plus efficace. Toutes ces données, si elles ne sont pas protégées, peuvent devenir visibles et accessibles à n'importe qui, et produire des effets de bord néfastes. « Nous avons beaucoup d'exemples depuis un an de défauts de protection des données. En parallèle, nous sommes dans un contexte de croissance extrêmement forte des cyberattaques. Tout cela pose des problèmes », explique-t-il. Pourtant, selon lui, « les solutions existent, et nous les occultons », et ce sera le but du séminaire de les présenter.

Enfin, au-delà de la simple confidentialité des données du grand public, il pointe particulièrement le respect du secret des affaires dans la question de la protection des données. « On l'oublie souvent, mais toute la matière grise créée par les entreprises doit aussi être protégée », insiste-t-il. Sans confiance, pas de business. C'est la base des échanges commerciaux. Si le numérique et plus particulièrement ces technologies veulent croître, il nous faut progresser là-dessus. Il rappelle qu'une technologie n'est jamais neutre.

2/ Le résumé des différentes interventions de la journée

2.1 - Les conditions organisationnelles d'une confiance vérifiables dans les systèmes d'IA

Par **Dominique Boulier,** Science Po

Ressource ici

Dominique Boulier est sociologue, spécialisé dans les organisations et les technologies du numérique. Il revient lors de sa présentation sur le concept de « confiance vérifiable », une confiance qui se

situerait entre la transparence totale et la confiance aveugle. « La défiance absolue n'est pas non plus vivable », décrit-il. Sa présentation viendra évoque les conditions de création de la confiance.

La première est la notion de « convention » entre différents acteurs. Les conventions permettent de poser les bases de la confiance. Tout part des organisations et des modes d'organisation qui permettent de créer une économie et des relations d'échanges entre les parties. Cela nécessite des standards et un « environnement sécurisé de convention. » Exemple de standards : partager une terminologie commune entre tous les acteurs. Avec ici, un hic, concernant l'intelligence artificielle en B2C : le fait qu'on ne peut forcer un utilisateur à utiliser une terminologie spécifique.

Mais la convention doit aussi permettre le contrôle. Les acteurs doivent être possiblement contrôlés, e de manière efficace. Si cette éventualité n'existe pas, la confiance se délitera. Le système d'organisation doit donc permettre d'effectuer ce contrôle.

Dans un deuxième temps, il décrit les conditions du développement de l'IA générative sans convention et sans confiance – ce qui semble être le cas des conditions actuelle. Dominique Boulier revient sur l'histoire du lancement du ChatGPT, en 2022, qui ressemble à un phénomène de création de dépendance, dans « la logique du dealer ». Une mécanique bien connue des géants du numérique. « On amorce le marché par la gratuité, sans aucune concertation ni contrôle de la mise du produit sur le marché », détaille-t-il. Se met alors en place un accès public immédiat, sans aucune régulation ni concertation. En ce qui concerne ChatGPT, se pose par exemple la question du « pillage » des données sources, celles ont permis d'établir le système numérique (ici, la presse et les artistes). Cela a été effectuée sans aucun moyen de contrôle ni de transparence. Ainsi le public doit faire aveuglément confiance au système, sans que le droit n'ait son mot à dire. D'un point de vue plus « culturel », il insiste sur le fait que le marché crée une « urgence » à adopter la technologie. « Le grand changement, avec l'IA, c'est l'immédiateté de la technologie, qui s'inscrit dans une idéologie de « disruption », et c'est cette logique qu'il faut contrer », argue-t-il donc.

Dans une troisième partie, Dominique Boulier donne des clefs pour former des organisations plus appropriées, et revient sur les conditions d'établissement de la confiance entre l'IA et les humains. Il rhabille d'abord les économistes dont selon lui, toute l'histoire de la discipline consiste à chercher à « se débarrasser du social. » Il estime que l'économie est une « discipline hors sol qui s'émancipe des conditions réelles de la vie », et fait un parallèle entre l'établissement des modèles d'IA, qui sont des systèmes de calcul. Par le passé, les systèmes d'IA symboliques (établie par des règles), nécessite de décrire le monde « Cela prenait un temps fou et demandait beaucoup d'experts, sans faire l'économie de leur propre rapport au monde », décrit-il. Aujourd'hui, les modèles connexionnistes (par apprentissage) sont construits avec tout ce qui vient, et les modèles sont limitées par les données qu'on y intègre.

La solution consiste à réfléchir les systèmes d'IA et les systèmes organisationnels en même temps. Dominique Boulier présente ainsi trois critères : des systèmes cohérents, des systèmes explicites, et des systèmes conformes aux valeurs. Ainsi les systèmes doivent engager des responsabilités, et ce, dès leur création. C'est ainsi qu'il revient sur le protocole de contrôle, qui doit être travailler et travailler la chaîne de responsabilités. Il avance alors un argument de poids : pourquoi le véhicule autonome stagne à l'heure actuelle ? Car, si techniquement, il est valide, il n'a pas été pensé dans le même écosystème que celui dans lequel il doit évoluer. Car les écosystèmes sont immodélisables. Idem pour toutes les innovations de « smart city », dont on n'entend plus parler. C'est ainsi qu'il faut intégrer les assureurs dans la boucle. « Qui s'est posé la question anthropologique, quand on crée des IA qui font parler les morts, des boucles de déni du deuil et de leurs effets sur l'humain ? », argue-t-il. Et le sociologue s'interroge sur le fait que des idées « tordues » puissent devenir « sympas », auprès des

médias ou du grand public. Même s'il faut admettre que l'instabilité de l'innovation « permanente » est en tension avec les conventions qui viendraient la cadrer. Et c'est là tout le point : arriver à concilier les deux.

Enfin, il termine en estimant que le point de visée doit être le design participatif. Car il déplore qu'aujourd'hui on ne puisse plus ouvrir le capot des systèmes pour les comprendre, et pour avoir un impact dessus. Donc le risque peut venir de partout.

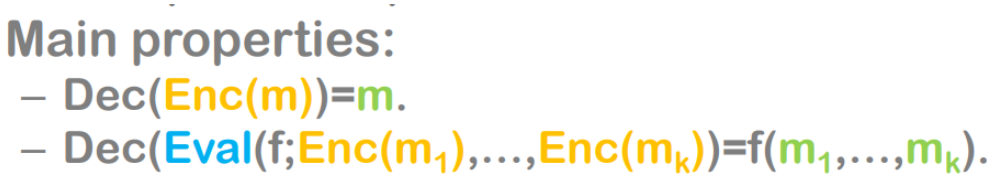
2.2 - A gentle Overview of FHE and some of its application

Par **Renaud Sirday,** CEA

Ressource ici

Renaud Sirday est chercheur au CEA et va présenter le fonctionnement du Fully Homomorphic Encryption (FHE), ainsi que certaines de ses applications. Il revient brièvement sur son histoire. Le chiffrement entièrement homomorphe a énormément avancé à partir des années 2010, notamment avec IBM.

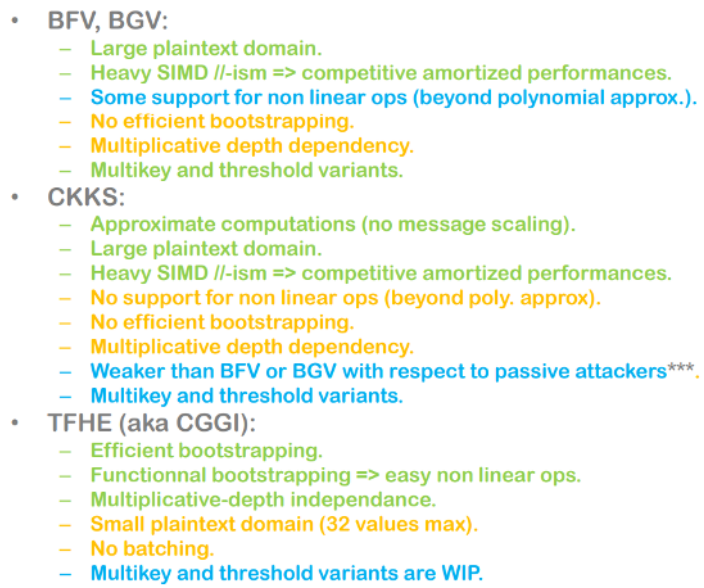
Le principe du chiffrement homomorphe est assez simple. Il consiste à chiffrer des données, à pouvoir exécuter des opérations sur ces données chiffrées, et par le même procédé de déchiffrements, obtenir le résultat des opérations comme si elles avaient été effectuées sur les données de départ. On peut ainsi, en ne travaillant que sur des « chiffrés », obtenir des résultats identiques à ceux dans l'espace « non chiffrés ». « On peut ainsi travailler en aveugle sur des données et aboutir à des résultats chiffrés possiblement déchiffrables », détaille Renaud Sirday. Ce qui en matière de données personnelles, est extrêmement confortable… Une propriété qui se matérialise mathématiquement ainsi :



Seul souci : le chiffré est beaucoup plus gros que le déchiffré. Il existe donc un coût computationnel à l'opération. Il faut donc atténuer ce coût.

Le concept permet ainsi d'établir des opérateurs (multiplication, ou autre) de les exécuter dans l'espace chiffré, et de retourner ensuite dans l'espace déchiffré. Seul problème, surtout pour les multiplications, et les systèmes d'équations linéaires, il peut y avoir du bruit lors de l'opération de déchiffrement. Le but consiste donc à tenter de minimiser ce bruit. Il faut l'absorber comme on peut, en choisissant le paramètre dans le chiffrage qui permet de diminuer le bruit.

Il rentre alors dans les différents « types » de chiffrement homomorphes qui existent, avec chacun leurs propriétés : BFG, BGV, CKKS, TFHE.



Il donne ensuite un exemple de « Data Privacy in training », via deux serveurs qui ne partagent aucune de leurs données. Le FHE permet de mettre en place un « apprentissage fédératif », qui offrira un modèle construit la somme de modèles partiels, avec chacun son chiffrement. Il détaille alors les caractéristiques plus techniques des calculs. Sur l'exemple qu'il donne, le temps de calcul pour chiffrer par FHE n'augmente que de 0,2% à 1,1%. Le temps de chiffrement est donc, selon lui, négligeable.

Enfin, il résume ce qu'il faut retenir du chiffrement homomorphe :

C'est un chiffrement probabiliste, dont la sécurité est démontrable, et qui peut s'appliquer sur tout type de données. Mais l'introduction de bruit dans l'opération de déchiffrement peut induire des questions sur la qualité des résultats. Il prévient que le chiffrement ne correspond pas forcément à l'image que l'on s'en fait. Et qu'il ne faut pas oublier que les algorithmes réalisent toujours a minima, leur pire scénario.

2.3 – Technique de protection des données privées dans le contexte des marchés locaux d'énergie

Par **Victor Languille,** EDF R&D

Ressource ici

Victor Languille traite des « marchés locaux d'énergie », nommée par l'Union Européenne, les « Communautés d'énergie ». Le terme décrit un ensemble d'acteurs qui produit et utilise de manière autonome son électricité. Ils gèrent leurs affaires en commun, leurs propres installations (panneaux solaires, batteries…) et peuvent donc avoir besoin de leur propre système d'information. Et on peut vouloir qu'à ces systèmes de production décentralisés correspondent des systèmes d'information décentralisés.

Les systèmes centralisés présentent trois types de problèmes : le contrôle, la vulnérabilité et la privacy.

Victor Languille présente alors les avantages des systèmes centralisés par l'exemple du Bitcoin, dans le système bancaire. Au lieu d'avoir une seule copie du registre des transactions stockées par une banque, on fait en sorte que n'importe qui puisse copier le registre et mettre en place des algorithmes

qui sont des protocoles de consensus, pour faire en sorte que les différentes copies du registre maintiennent les mêmes états au cours du temps, et au cours des différentes transactions. Cela résout mitigent les deux premiers problèmes : le contrôle et la vulnérabilité. En revanche pour la privacy, cela ne le résout pas mais cela l'empire : car in fine, tout le monde a accès aux transactions et est au courant de ce qu'il se passe.

Dans le système particulier de l'énergie, tout le monde va avoir accès à ce qu'on achète, et à qui. Ce qui peut poser des problèmes.

Given a certain y and a program P, allows a Prover to prove to a Verifier:

"I know x such that $y=P(x)$"

Le point consiste donc à résoudre la question de la privacy dans le cadre des systèmes décentralisés. Une solution existe : le Zero-Knowledge Proof, ou comment révéler qu'on a la solution à un problème sans révéler cette solution.

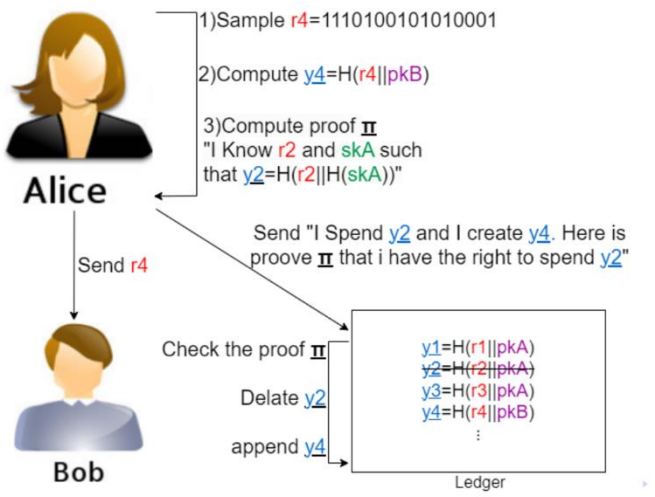
Victor Languille décrit alors le concept : c'est un protocole entre un « prouveur » et un « vérifieur » qui permettent d'exécuter :

Il prouve ainsi qu'il connaît Y étant donné P(x) sans jamais rien révéler du x en question. Pour cela il est très important qu'on atteste qu'étant donnée la preuve Pi, on ne sache rien du x en question.

Le but consiste alors à implémenter ce principe sur un registre de blockchain. C'est-à-dire que tout le monde puisse savoir que ce qu'il se passe sur le registre fonctionne bien, sans pour autant savoir ce qu'il se passe sur le registre. Pour cela, il faut établir une fonction H() (Hash), pour laquelle il est très facile étant donné x, de calculer H(x), mais très difficile étant donné H(x) de revenir à x.

Il décrit alors comment on arrive à créer des cryptomonnaies anonymes, en implémentant la fonction de hashage dans le protocole de transaction de coin sur la blockchain, entre les adresses publiques et les adresses privées.

La clef du raisonnement, consiste à faire en sorte que dans la transaction, un coin n'est pas transféré d'un portefeuille à un autre, mais le débiteur va supprimer un coin dans son portefeuille et le protocole d'échange va en créer un nouveau dans le portefeuille du créditeur. Le protocole peut être résumé dans le schéma suivant :



Enfin, pour finir, il présente comment ce mécanisme a été étendu aux marchés locaux de l'énergie, où aux coins sont ajoutés des tokens énergies, et où sont ajoutés également des protocoles d'enchères. In fine, les équipes ont réussi à créer une plateforme d'échange paire-à-paire d'énergie, avec des enchères, telle que la plateforme soit décentralisée, et tout en garantissant que personne ne puisse savoir en détail ce qu'il s'y passe, en garantissant l'anonymat des acteurs.

2.4 - Privacy-enhancing technologies: protection de la confidentialité des données de consommation d'électricité

Par **Benoit Grossin,** EDF R&D

Ressource ici La vidéo est disponible ici

Benoît Grossin travaille beaucoup sur le sujet des données et d'intelligence artificielle. Il revient sur l'équilibre qu'il faut trouver entre l'intimité des données à caractère personnel et l'usage qu'on a envie de développer avec.

La première chose à savoir, c'est que les données de consommation d'électricité sont des données à caractère personnel, car elles ont un pouvoir identifiant (la suite de votre consommation journalière sur une série de journées) au sens du RGPD. Et elles sont aussi considérées comme sensibles car elles peuvent révéler des informations sur la vie privée.

Cependant, comme l'explique Benoît Grossin *« l'urgence climatique et la transition énergétique doivent mobiliser toutes les ressources disponibles, a fortiori les données énergétiques. Cela est indispensable pour concevoir de meilleurs algorithmes de pilotage offre/demande, mieux cibler les actions de rénovation ou bien encore lutter plus efficacement contre la précarité énergétique. »*

La problématique consiste donc à résoudre le dilemme pour concilier les besoins croissants d'utilisation des données énergétiques et la protection de leur confidentialité ?

Le projet consiste donc à travailler sur les Privacy Enhancing Technologies, c'est-à-dire qui permettent de collecter, processer, analyser et partager des données tout en garantissant la protection de leur confidentialité. Il va en présenter deux.

La première est la confidentialité différentielle, qui consiste en un floutage de l'information. Elle fonctionne sur des données agrégées. L'autre technologie consiste à créer des données synthétiques qui « ressemblent » aux données de départ, et sur lesquelles on va pouvoir travailler.

La confidentialité différentielle consiste donc à ajouter du bruit dans les données agrégées. Cette méthode a l'avantage d'être pilotable, et elle s'adapte à la donnée qu'on veut protéger. Nous n'avons pas besoin de définir un bruit « a priori ». C'est la méthode qui va juger du risque de réidentification des données individuelles. L'autre point, est que les mathématiques permettent de garantir la protection de la donnée. En revanche, la méthode n'est pas « intuitive », et elle a dû être adaptée pour s'appliquer à des séries temporelles.

Il détaille ensuite le mécanisme du paramètre « epsilon », qu'on appelle le « budget privacy », qui est un paramètre qui va définir le degré de protection, et qui varie entre zéro et + l'infini. Plus on se rapproche de zéro plus la protection est élevée. « Mais plus on crée de bruit, et plus on perd la fidélité de l'information », explique-t-il.

Après plusieurs années d'affinage du modèle, voici ce à quoi a abouti EDF. En bleu, la courbe réelle que voulait protéger les équipes. Trois ans ont été nécessaires pour paramétrer convenablement le paramètre epsilon, et de l'adapter, afin de ne pas perdre le côté informatif du résultat et pouvoir en faire quelque chose.

Implémentations naïves de la DP **Implémentations optimisées de la DP**

Benoît Grossin revient alors sur la deuxième technique, la création de données synthétiques. Il décrit d'abord un système de génération de données synthétique. Il se base sur un modèle de Deep Learning, GAN, avec un « discriminateur », qui va devoir chercher à différencier les données synthétisées des données réelles. S'il y arrive, c'est que le modèle n'est pas assez proche de la réalité. Il revient ensuite sur un partenariat avec Enedis, qui a consisté, via un modèle de machine Learning, à générer des courbes fictives mais réalistes de consommation, pour pouvoir ensuite travailler dessus.

Leurs avantages ? Elles sont configurables, économiques, et massivement disponibles. En revanche, difficile de savoir si elles respectent véritablement la privacy. Cela doit amener à des travaux spécifiques selon le cadre dans lequel elles sont créées et utilisées.

Ainsi, pour produire des bonnes données synthétiques, il faut vérifier si elles sont fidèles, utiles et si elles respectent convenablement la privacy.

2.5 - IA en santé : anonymiser des données cliniques pour optimiser des parcours de soin en confiance

Par **Olivier Breillacq,** Octopaz

Ressource ici

Olivier Breillacq est le fondateur de la société Octopaz. Elle est spécialisée dans la synthèse de données à des fins d'anonymisation. Il présente ainsi sa solution et le contexte dans lesquels elle répond aux besoins des organisations.

Aujourd'hui, 75% des données sont collectées à des fins d'usages secondaires. Et le RGPD ne règle absolument pas toute la question. Le principe de génération de données de synthèse permet de protéger la confidentialité des données tout en garantissant leur qualité.

Le principe repose sur une « avatarisation » des données. C'est une méthode qui se différencie de la méthode GAN (citée plus haut).

Elle commence par une projection multidimensionnelle. Les données originales sont projetées dans un espace multidimensionnel approprié à l'aide de techniques de réduction des dimensions telles que l'analyse factorielle des données mixtes (FAMD), l'analyse en composantes principales (ACP) ou l'analyse des correspondances multiples (ACM). Chaque transformation doit être réversible. Les individus sont ainsi transformés en coordonnées réduites dans une espace numérique structuré. Une deuxième étape consiste à calculer les plus proches voisins de chaque individu dans cet espace. Cela définit une zone locale entre chaque individu.

Pour chacune de ces zones locales sont ensuite simulées des nouvelles coordonnées pseudo-aléatoires. Cette projection mêle différents paramètres : la distance entre les points d'origine, mais aussi un poids aléatoire exponentiel. Cela permet aux simulations non-déterministes d'être un processus irréversible afin de préserver la vie privée.

Ensuite, partant de cette distribution, on revient à l'espace de départ, les coordonnées de l'avatar sont inversées pour revenir à l'encodage original, en conservant le type des attributs originaux (catégoriques, numériques, etc.). Sans pour autant être en mesure de revenir à l'individu de départ.

Est ensuite calculé un « paramètre de protection de la vie privée », défini par le Comité européen de la protection des données. Il prend en compte trois critères : l'individualisation, la corrélation et l'inférence.

La méthode des avatars présente différents avantages : elle permet de contrôler la confidentialité, de garder la main sur la qualité de la structure de données originales. *« Elle permet d'anonymiser tout en conservant la qualité et la structure originale de l'information, conditions indispensables pour assurer la reproductibilité des résultats d'une étude ou améliorer l'efficacité d'une IA »,* indique Olivier Breillacq.

2.6 – Le chiffrement homomorphe, la solution pour la confidentialité des données en IA et blockchain

Par **Andrei Stoian,** Zama

Ressource ici La vidéo est disponible ici

Andrei Stoian a fondé la société Zama, qui est leader dans le domaine du Fully Homomorphic Encryption (FHE), le cryptage entièrement homomorphique. Sa présentation consistera à expliquer le concept, les avantages et les potentialités du cryptage homomorphique appliqué à l'IA et surtout à la blockchain.

Zama emploie 75 employés, dont 40 doctorants-chercheurs. Tous les codes sont en open-source, ce qui permet d'être plus transparent, et de faciliter le test des produits par les entreprises. Elle rassemble une communauté de 3000 développeurs, qui contribuent à l'écosystème et a levé 70 millions d'euros. Zama a été fondée par Pascal Paillier et Rand Hindi en 2020. Un autre cryptographe très connu les a rejoints en 2022 : Nigel Smart.

Andrei Stoian précise qu'il ne reviendra pas sur la partie technique qui a été présentée ce matin, par Renaud Sirday, du CEA. Il précise que le milieu change encore très vite. Il rappelle que les besoins en protection des données s'est accentué avec l'utilisation massive des services Cloud. Quand les données

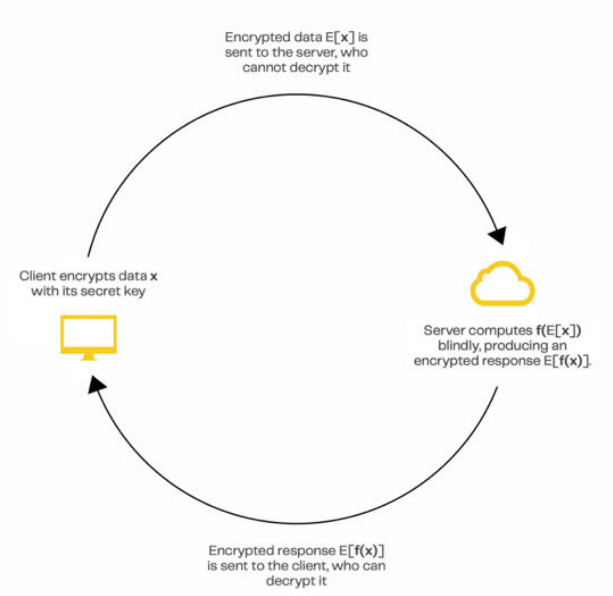
étaient stockées par les entreprises, il suffisait de couper internet, pour en assurer la protection, mais aussi car la réglementation a évolué massivement ces dernières années. Et le chiffrement homomorphe vient répondre à ces besoins.

Il revient d'abord sur les questions de confidentialité liée à l'utilisation de l'IA et notamment ChatGPT, et à celle de la blockchain. Dans ce dernier cas, tout est public, seule la pseudonymisation des utilisateurs garantie une part de confidentialité. Il évoque ensuite les avantages : règlement rapide (un milliard de dollars peut-être transférer en 10 minutes), atomicité (l'argent ne peut pas se perdre), la réglementation est programmable (pas plus de 200 euros par jour) et l'interopérabilité des systèmes. On pourra y brancher des systèmes qui n'y sont pas connectés pour faciliter les échanges entre différents types d'actifs.

En revanche, plusieurs inconvénients subsistent : le vol, la surveillance qui peut amener à une manipulation du coût des transactions.

Il décrit alors le fonctionnement de l'échange des données à l'heure actuelle, où le chiffrement n'a lieu que lors du transfert de l'information. Avec le FHE, on peut appliquer des programmes sur les données chiffrées, nous n'avons plus besoin de déchiffrement intermédiaire.

Le mécanisme est résumé sur le schéma ci-dessous :



Dans le cas particulier de l'IA, le serveur ne stocke que des données chiffrées. Ainsi, en cas de piratage, les attaquants ne pourront rien faire des données, la clef de déchiffrement étant stockées, elle, côté client. Le FHE favorise également la collaboration confidentielle, où différents acteurs peuvent renforcer les modèles en mettant leurs données en commun, afin d'optimiser les prédictions. Cette mise en commun s'affranchit de tout protocole sécuritaire, car les données échangées ne sont que les données chiffrées, dès qu'elles partent du serveur Zama.

Andrei Stoain présente alors différents cas d'application, pour la finance et pour la santé.

Puis il présente ensuite le fonctionnement pour l'application à la blockchain. Le FHE va principalement servir à masquer le montant, la partie la plus sensible des transactions.

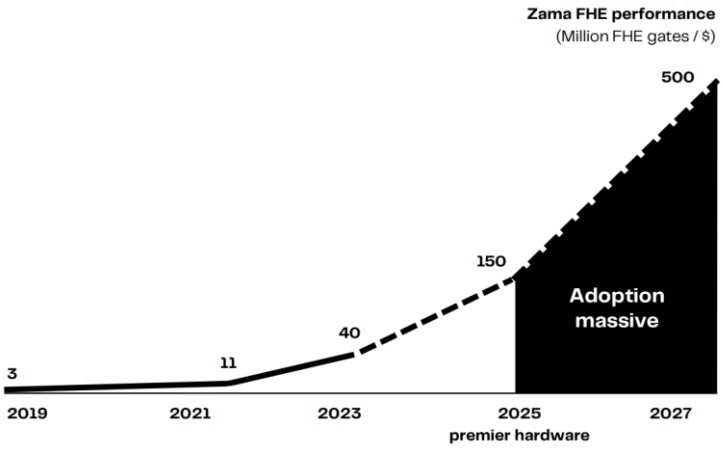
En masquant ainsi cet élément structurant du principe de la blockchain, le FHE débloque de nouveaux cas d'usage :

- La tokenisation : Gestion et transactions des actifs tokenisés sans dévoiler les montants,
- Les enchères à l'aveugle : Faire une offre sans dévoiler son montant et cacher le gagnant de l'enchère,
- Electronic Cash : gérer des transactions anonymes,
- Vote confidentiel : afin d'empêcher la corruption des électeurs,
- Identité chiffrée : cela permet de vérifier l'identité des personnes, ou pour contrôler l'accès à des applications décentralisées.

Andrei Stoian revient également plus particulièrement sur le travail en cours des banques centrales, et de leurs intérêts pour le FHE.

Enfin, pour conclure, il revient sur les enjeux techniques de cette méthode de chiffrement : elle est de plus en plus rapide. En 2024, les smart contracts par FHE sont de l'ordre de 5 transactions par secondes. Pour les petits modèles d'IA, la FHE induit une latence de l'ordre de quelques secondes.

L'évolution des performances est présentée dans le graphique ci-dessous :



2.7 – Virtual & Invisible Private Network (VIPN) : Enjeux et cas d'usages du premier réseau d'Invisibilité sans tiers de confiance sur Internet

Par **Baptiste Polvé,** co-fondateur et CTO, Snowpack

Ressource ici La vidéo est disponible ici

Snowpack est une jeune pousse dont le but est de se focaliser sur la sécurité du transfert des données, afin de ne pas pouvoir tracer qui parle avec qui. Le principe de la technologie a été inventé en 2017, avec des chercheurs du CEA. Depuis, elle a gagné de nombreux prix, dont la médaille d'or du forum cyber.

Le postulat de départ consiste à établir qu'à partir du moment, où sur internet, on sait qui parle avec qui, un catalogue de menaces existe. « Sur internet, tout passe par le protocole IP, qui a besoin de savoir qui parle avec qui pour que ça fonctionne », explique Baptise Polvé. Les portes d'entrées pour

les assaillants sont les ports ouverts, sur les serveurs. D'autre part, des acteurs externes vont fournir des technologies de sécurisation qui sont soit involontairement mauvaise, soit même, volontairement mauvaise – des exemples existent outre atlantique – afin de diminuer volontairement le niveau de sécurité, même lorsqu'il y a du chiffrement. Le principe de Snopack consiste à ajoute une « couche de neige » au dessus des systèmes pour éviter de percevoir qui parle avec qui, et de pouvoir localiser les points d'entrée sur les systèmes d'information. Concrètement : éliminer les informations des métadonnées, et faire en sorte de pouvoir exposer des informations sans avoir à ouvrir des serveurs, sans avoir à ouvrir des ports sur internet, et sans avoir besoin de faire confiance à des tiers.

Pour cela, la jeune pousse a développé une technologie qui s'appelle Virtual and Invisible Private Network. Elle permet de masquer des activités de connexion (pour une personne en opération, par exemple), mais aussi d'avoir accès à des services invisibles sur internet.

Comment ça fonctionne ?

Snowpack utilise pour cela un réseau de serveurs distribués (comme le réseau Tor qui a été développé par l'armée américaine). Une autre clef s'appelle la fragmentation (ou floconisation, pour la jeune pousse). Elle consiste à prendre un paquet d'IP, à en oter les adresses IP sources, et à les passer dans un XOR, avec des aléatoires, ce qui va donner des alétoires complémentaires, qui eux, ne seront pas déchiffrables, pris indépendemment. C'est le principe du « secret sharing », il est impossible de savoir si ce qu'on retrouve à la fin est bien ce qu'on cherchait on départ.

La société a aussi mis en place un mécanisme d'auto découverte, qui permet à deux entités de communiquer au milieu du réseau, sans connaître la demi route qui a amené chacune des entités ici. Pour cela il faut garantir que personne ne puisse se mettre au milieu et intercepter les échanges.

Tout cela induit une moindre dépendance à la souveraineté des données, ou permet de gagner en résilience en distribuant les jeux de données chez différents fournisseurs. « On mixe on mixe, à la fois les serveurs et les technologies », détaille-t-il.

Ainsi, plutôt que d'aller sur du chiffrement, Snowpack permet d'aller davantage sur de la fragmentation des échanges sur le réseau. Le chiffrement repose ainsi davantage sur les flux, plutôt que sur les opérations exécutés sur le device.

La société est en train de prouver – avec publication prévue – que la sécurité du chiffrement du réseau est garantie. Car si le système tombait, il se résumerait à résoudre un problème de système de mot de passe. « Et à partir de 50Mbits de flux, il faudrait plusieurs milliards d'années pour le résoudre », avance Baptiste Polvé.

Le CTO présente alors différents cas d'usage de sa technologie, et notamment des besoins d'anonymisation, que ce soit : pour de la protection de la vie privée, pour de la protection de données business, pour garantir les droits humains ou encore d'autres catégories (liberté d'expression, de communication…)

Point important : la société a bien conscience que développer des réseaux d'anonymsation peut amener des dommages collatéraux importants, comme favoriser des actités terroristes ou illégales. Elle veut avant tout avoir un impact positif. Mais elle a développé une offre pour les particuliers gratuites, et cette offre est essentiel, car les particuliers, pour des activités à faible valeur ajouté, vient enrichir le système est créer du flux, qui permet de cacher les autres. Comme les autres réseaux distribués, c'est la masse qui fait partie intégrante du système pour diluer également l'information.

Il détaille ensuite les mécanismes de responsabilisation, notamment quand la justice fait des demandes d'identification, pour les particuliers, comme pour les entreprises.

Enfin, pour conclure, il résume tous les mécanismes d'anonymisation des réseaux et les compare :