RAPPORT

PROCEDES CRYPTOGRAPHIQUES AVANCES

ACN
Alliance pour la confiance numérique

ALLIANCE POUR LA CONFIANCE NUMERIQUE
WWW.CONFIANCE-NUMERIQUE.FR

Table des matières

Remerciements

Ce rapport a été préparé par l'Alliance pour la Confiance Numérique (ACN)
à la demande de la mission Prenium.

L'Alliance pour la Confiance Numérique (ACN) tient à remercier les personnes suivantes pour leur participation à la préparation de ce rapport technique :

- Maria CHRISTOFI (Oppida) ;
- Guy de FELCOURT (Admissions Technologies) ;
- Alban FERAUD (IDEMIA) ;
- Christophe CIANCHI (BCA) ;
- Aline GOUGET (Thales) ;
- Sylvain GUILLEY (Secure-IC) ;
- Laurent HENOCQUE (Keeex) ;
- Pascal PAILLIER (CryptoExperts) ;
- Béatrice PEIRANI (Thales) ;
- Jean-Pierre QUÉMARD (KAT) ;

Introduction

Ce rapport présente les différentes technologies cryptographiques existantes ou en cours de développement qui permettent de mettre en œuvre les fonctionnalités d'identification et d'authentification nécessaires au déploiement de l'identité numérique dans une société numérique. Il n'y a pas de solution unique et générale à ce besoin car les problématiques sont variées en fonction des cas d'usages : identités régaliennes, e-commerce, e-administration, protection de données personnelles, … et selon les besoins opérationnels : ressources nécessaires, coût de la solution et de sa mise en œuvre, résistance aux attaques, compatibilité et interopérabilité.

QUELS NOUVEAUX BESOINS DE SECURITE POUR L'IDENTITE NUMERIQUE DE DEMAIN ?

Les tendances lourdes sont :

- Non-traçabilité et mise en œuvre de techniques d'anonymisation puissantes ;
- Protection des données personnelles en demande sociétale forte, renforcée par l'entrée en vigueur du RGPD ;
- Contrôle et souveraineté des données, lors du stockage et traitement des données en nuage ;
- Résilience contre les cyberattaques et sécurité à long terme ;
- Compatibilité ascendante et descendante des technologies mises en œuvre ;
- Sécurité numérique et nomadisme technologique.

BENEFICES DE LA CRYPTOGRAPHIE

Les bénéfices de la cryptographie sont : sécurité mesurable, démontrable et ne reposant sur aucune hypothèse sur l'environnement, c'est une technologie fiable, scientifiquement bien comprise et largement normalisée.

Des algorithmes peuvent être conçus pour répondre à de nouveaux besoins de sécurité dès lors qu'ils sont clairement définis, les possibilités mathématiques sont presque sans limites si ce n'est les difficultés d'implémentation.

Mais cela nécessite un travail de recherche fondamentale afin de valider de nouveaux algorithmes, protocoles et dispositifs matériels ainsi qu'un effort important dans le domaine de la normalisation afin en particulier de permettre l'interopérabilité et la certification des systèmes déployés.

QUELS NOUVEAUX BESOINS DE SECURITE POUR L'IDENTITE NUMERIQUE DE DEMAIN ?

Besoins	Procédé cryptographique	Avantages
Non traçabilité et techniques d'anonymisation	FIDO	*Cross domain anonymity* // pas de collusion possible entre fournisseurs de services pour "profiler un utilisateur"
Non-traçabilité et techniques d'anonymisation	Blockchain	Non-traçabilité (pas de base de vérification centrale)
Non-traçabilité et techniques d'anonymisation	Accréditations anonymes ou ABC Chiffrement basé sur l'identité et sur les attributs (IBE, ABE)	Anonymisation accrue car permet de s'intéresser aux attributs des personnes et non à leur identité complète
Résilience contre les cyberattaques et sécurité à long terme	Cryptographie résistante à l'ordinateur quantique	Protection contre le vol d'identité via un moyen permettant de réaliser de la cryptographie de manière sécurisée à long terme
Contrôle et souveraineté des données, lors du stockage et traitement des données en nuage	Chiffrement homomorphe	Permet de chiffrer des données de sorte à garantir leur confidentialité tout en permettant leur traitement par des tiers
Contrôle et souveraineté des données, lors du stockage et traitement des données en nuage	Nouvelles technologies autour du zero-knowledge	Contrôle d'accès à des données stockées en nuage
Contrôle et souveraineté des données, lors du stockage et traitement des données en nuage	Cryptographie à seuil	1. Protection contre le vol d'identité via un mécanisme renforcé d'authentification et de chiffrement reposant sur une résilience accrue 2. Mise en responsabilité des fournisseurs de services en permettant un contrôle a priori de ses actions
Sécurité numérique et nomadisme technologique	Cryptographie en boîte blanche	Protection contre le vol d'identité via un moyen permettant de réaliser de la cryptographie de manière sécurisée dans un environnement quelconque

Blockchain

DESCRIPTION DE LA TECHNOLOGIE

La chaîne de blocs (de l'anglais « blockchain », tellement utilisé que nous utiliserons généralement le terme anglais)[1] est une technologie, initialement utilisée dans le contexte des cybermonnaies (traduction française officielle de l'anglais « *cryptocurrency* »), afin de conserver la trace irréfutable et inviolable de transferts d'actifs numériques interdisant la double dépense. La particularité de la blockchain Bitcoin fondatrice de ce modèle est l'absence de la nécessité d'un *tiers de confiance,* i.e. une entité formelle et centralisée responsable de contrôler toute transaction effectuée. La blockchain Bitcoin est en effet opérée en pair à pair, et de fait se trouve normalement impossible à arrêter ou censurer, de la même manière que le système d'échange de fichiers BitTorrent (utilisé dans les échanges entre pairs : *peer to peer*).

Une blockchain peut être vue comme un registre numérique horodaté et inviolable qui enregistre les transactions effectuées et permet de garder un historique de ces échanges depuis sa création. Ce registre est répliqué par ses différents utilisateurs, sans entité centrale. Ceci permet à chaque utilisateur de cette blockchain de vérifier la validité de la chaîne (et de toute transaction), et de construire localement une base de données représentant l'état instantané de la chaîne pour répondre rapidement à des requêtes.

Il existe plusieurs types de blockchain :

- Les blockchains publiques ouvertes à tous (par exemple : bitcoin, Ethereum, Ripple)
- Les blockchains privées dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs (par exemple : R3 CEV ou Hyperledger Fabric d'IBM). Parmi ces dernières, des fonctions de contrôle d'accès permettent de les qualifier de « permissionnées ».
- Les blockchains hybrides (ou de consortium) qui peuvent utiliser les deux types d'accès, certaines données peuvent être consultées publiquement, tandis que d'autres ne sont disponibles que sur un réseau privé. Par exemple, la consultation peut être publique, alors que la validation est uniquement accessible en mode privée.

Le principe d'une blockchain est que toutes les transactions effectuées entre utilisateurs du réseau sont regroupées par bloc. Chaque bloc, contenant un

[1] Vocabulaire informatique normalisé par l'académie française publié au JORF n°0121 du 23 mai 2017, texte n° 20 : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000034795042

ensemble des transactions, est validé par les nœuds du réseau en suivant les règles établies par le *consensus* de cette blockchain. Une fois que le bloc est validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est maintenant visible à l'ensemble du réseau et son récepteur peut recevoir et valider cette transaction[2].

Le consensus, dont on a parlé précédemment, correspond à un ensemble de règles assurant le bon fonctionnement de la blockchain, y compris les techniques devant être mises en œuvre afin de valider une transaction. Le choix du protocole de consensus est essentiel pour construire la confiance dans un système où plusieurs parties doivent coopérer sans avoir d'autorité hiérarchique commune. Plusieurs choix sont disponibles pour ces techniques :

- *Proof of work*, preuve de travail, basée sur la capacité de résoudre de problèmes algorithmiques (par exemple, Bitcoin utilise cette technique). Une preuve de travail est le résultat de calculs arbitrairement longs dont la vérification est extrêmement rapide.
- *Proof of stake*, preuve d'enjeu ou de participation, basée sur la preuve de possession d'une certaine quantité de cybermonnaie (par exemple, NxT)
- *Proof of elapsed time*, preuve de temps passé, basée sur le temps d'attente avant d'avoir une réponse par un TEE (par exemple, Sawtooth Lake d'Intel)
- *Proof of burn*, basée sur le principe de détruire une partie de ses tokens afin de pouvoir écrire des blocs
- *Proof of memory* : preuve de l'utilisation d'une quantité donnée de mémoire vive.
- *Practical Byzantine Fault Tolerant*
- …[3]

Les hypothèses de sécurité et de confiance varient d'un protocole de consensus à l'autre. Par exemple, dans le cas du protocole *Proof-of-work* utilisé par Bitcoin, on observe qu'il existe des stratégies rationnelles dites de « *selfish mining* » qui permettent d'optimiser les gains obtenus par un pool de mineurs en fonction de la force de calcul de ce pool qui n'est pas forcément élevé ainsi que de la capacité de contrôler la transmission des données sur le réseau. La localisation des forces de calculs sur le réseau est donc un élément important à prendre en compte dans le choix d'un algorithme de consensus. Une fonction clé de la preuve de travail utilisée par Bitcoin est que sa complexité s'adapte automatiquement à la puissance de calcul délivrée par le réseau de mineurs pour garantir statistiquement la production d'un bloc toutes les dix minutes, ce qui incite les mineurs à se regrouper en pool. Dans le choix d'un algorithme de consensus, il est important de prendre en compte le type de blockchain (public, privé, consortium). Le protocole

[2] Dans le vocabulaire des cybermonnaies, les fonds transmis et non encore réutilisés constituent une « sortie de transaction non dépensée » (UTXO – Unspent Transaction Output). La double utilisation de ces fonds est garantie comme impossible.
[3] Et de nombreuses autres, selon de multiples variations https://en.wikipedia.org/wiki/Proof-of-work_system

de consensus proof-of-work (utilisé par Bitcoin et nécessitant de forte capacité de calculs) ainsi que le protocole *proof-of-stake* ne paraissent pas être adaptés aux modèles privé et consortium dans les cas où les différentes entités ont un poids équivalent. Une bonne compréhension de la sécurité des différents protocoles de consensus est importante pour pouvoir construire de la confiance dans les technologies blockchain.

PREAMBULE : PRATIQUE QUOTIDIENNE DE L'IDENTITE NUMERIQUE ET DE L'AUTHENTIFICATION

L'identité numérique combine deux problématiques : identifier un participant (qui est cette personne ? – par exemple par un nom complet, un pseudo), et authentifier (cette personne est-elle qui elle prétend). On considère habituellement quatre moyens de s'authentifier[4] :

- On connait un secret ou une donnée considérée comme telle (mot de passe, date de naissance, …).
- On possède un document (passeport).
- On répond à des critères donnés (biométrie, ADN…).
- On sait faire quelque chose (signature manuscrite).

Les services en ligne des banques et assurances utilisent depuis longtemps des éléments de l'identité complète (nom de la rue, date de naissance) comme un secret permettant une identification suffisante lors d'une interaction par téléphone, après un accès dont le seul élément probant est au départ le numéro de téléphone appelant.

Les usagers ont aujourd'hui massivement recours au service d'oubli de mot de passe pour accéder aux services qu'ils consomment. La procédure du « mot de passe oublié » utilise souvent l'adresse mail comme preuve de l'identité de la personne. Ceci signifie que les paramètres d'accès à un compte mail sont utilisés non seulement pour l'accès à la messagerie, mais est aussi un élément permettant de prouver l'identité d'une personne face à une demande de renouvellement d'accès à un autre service.

En Afrique, le compte Facebook est parfois utilisé comme preuve d'identité, la capacité à émettre un message provenant d'un compte donné étant considérée comme preuve suffisante que l'interlocuteur est bien la personne que décrit ce compte.

L'utilisation de la preuve d'accès à un compte pour accéder à un autre compte relève de la même logique lorsqu'un site propose de s'y connecter avec son compte Facebook, ou dans un cadre plus formel via France Connect[5].

---

[4] Authentification Wikipedia : https://fr.wikipedia.org/wiki/Authentification
[5] https://fr.wikipedia.org/wiki/FranceConnect et https://franceconnect.gouv.fr/

Il est intéressant de questionner la nature de la preuve obtenue dans ces cas « relais ». On y voit qu'authentifier quelqu'un n'est pas qu'une simple opération technique. Cela suppose aussi une confiance suffisante dans la preuve d'une non-usurpation : est-il possible de produire les preuves attendues tout en se faisant passer pour quelqu'un d'autre ? On voit l'importance de cette question pour un examen scolaire ou une opération bancaire majeure.

On utilise ici comme preuve d'identité en dernier ressort la preuve de contrôle du service ou système dont on pense que l'usager ne partagera jamais les identifiants, à cause de la force de l'investissement personnel et du risque réputationnel qu'il y aurait à faire ce partage dans le cas Facebook, et à cause du danger représenté par un accès centralisé à d'autres services dans les autres cas (France Connect). Une personne confiera plus facilement sa carte de crédit avec le code PIN que l'accès à son compte Facebook. En quelque sorte je peux croire que celui qui contrôle ce compte email ou Facebook est bien qui il prétend parce que je suppose que personne de sensé ne partagerait une telle intimité, fût-ce pour frauder un examen.

Cette dimension de l'authentification associée à une garantie suffisante que l'opérateur n'aurait jamais confié ses identifiants à un tiers est absente de tous les dispositifs numériques dénués de charge affective. Toutefois, il est possible comme on le verra plus bas d'en combiner les effets avec une identité numérique reposant sur la blockchain.

IDENTITE NUMERIQUE ET BLOCKCHAIN

Dans le monde réel, s'identifier consiste à prouver que l'on est en possession de documents matériels uniques infalsifiables, comme un passeport ou un permis de conduire, ces documents étant produits de façon suffisamment sécurisée par une autorité (par l'utilisation de techniques d'impression sophistiquées : filigranes, hologrammes…). La détention d'un objet unique inviolable est donc la preuve que je m'appelle 'Paul A'. Comme ce document porte une signature manuscrite, je peux en dernier ressort être invité à prouver que je sais reproduire cette signature. Ce deuxième facteur d'authentification est peu fiable et inutilisé aujourd'hui.

Les cybermonnaies. Les cybermonnaies ont initié leurs utilisateurs au transfert de valeur protégé par la partie privée d'une bi-clé, constituée d'une clé publique et d'une clé privée. La cryptographie de Bitcoin notamment utilise la cryptographie à base des courbes elliptiques (et notamment la courbe secp256k1) produisant des clés de petite taille (quelques dizaines de caractères).

Cette cryptographie possède d'autres propriétés intéressantes :

- La courbe elliptique choisie possède des propriétés de linéarité permettant l'utilisation de schémas de production déterministe de clés (BIP32 :

http://bip32.org/#bip32 qui permet notamment de n'utiliser chaque adresse qu'une seule fois).
    - D'autres courbes, comme Curve25519, sont dotées de propriétés comparables et sont reconnues de bonne qualité, alors que d'autres, comme celles proposées par le NIST et l'ANSSI, n'ont pas ces propriétés.
- Il semble à ce jour, sous toutes réserves, que les adresses de paiement Bitcoin dérivées des clés publiques soient relativement immunes aux attaques quantiques grâce aux mécanismes utilisés (cascade de compressions et des fonctions de hachage).
- L'existence implicite d'un *bug bounty* de 100 milliards sur Bitcoin montre aussi la qualité et l'intérêt commun à la découverte anticipée de vulnérabilités.

En se référant à la classification précédente, la clé publique est un 'identifiant' et la clé privée est un 'secret'. Pour quelqu'un qui procède d'un outil ou programme de signature, la clé privée peut être utilisée pour créer une signature, et ainsi prouver que l'on sait 'faire' quelque chose. Enfin, dès lors que la signature est réalisée par un dispositif physique contenant et exploitant la clé privée, le cas échéant sans possibilité d'export de cette clé, le dispositif physique (clé Fido, Ledger, Trezor, Archos, HSM…), joue aussi le rôle d'un document, dont l'authenticité est vérifiée par la création d'une signature.

Le destinataire d'une transaction se désigne donc par une clé publique (par exemple une adresse de paiement Bitcoin). Seul le détenteur de la clé privée correspondante pourra utiliser les fonds transférés, au risque, en cas de perte qu'ils ne soient irrémédiablement perdus.

Ce principe se généralise aisément à des transferts d'actifs non financiers ou à des changements d'états dans des processus en général. Il est possible de la même façon de désigner l'état suivant, résultant d'une procédure ou d'une action, par une clé publique. Même si « l'état suivant » peut prendre plusieurs états, un seul et unique état pourra être validé avec la clé privée correspondante. Cet état sera considéré comme l'état suivant du processus.

Il y a plusieurs avantages à ce moyen d'opérer :

- La transaction est pseudonyme : il existe aucun moyen permettant de corréler une personne physique avec une transaction, sauf à pouvoir en remonter une chaîne dont une extrémité est connue.
- Les participants sont seuls détenteurs de la capacité à authentifier le destinataire : ils valident la clé publique selon des critères sociaux, sans intervention d'une autorité de certification

L'identité dans le modèle des cybermonnaies. Ce qui est intéressant dans le modèle de cybermonnaies est que l'identité du destinataire est gérée socialement.

La décision de transfert est prise par une personne (physique mais cela peut être automatisé) vers l'adresse de paiement d'une autre personne. La manière dont ce destinataire est connu, identifié et authentifié est gérée par l'émetteur selon les modalités requises par la situation.

Il en résulte un découplage entre l'identité réelle et le mécanisme d'identification et d'authentification lors du réemploi de la transaction, qui génère une situation dite *pseudonyme* : la chaîne de blocs garantit l'inviolabilité de l'échange et la disponibilité des produits sans que l'identité des participants ne soit connue. On parle de « pseudonymité » car en réalité il est rare que le début ou la fin d'une chaîne de paiements ne soit anonyme du fait du rapport à un moment donné au monde réel.

Quoi qu'il en soit, dépenser les produits d'une transaction en sa faveur ne requiert que la capacité à signer avec la clé privée correspondante à la clé publique d'identification.

Généralisation de l'identité sociale. L'approche actuelle de l'identité numérique repose sur des certificats générés de façon pyramidale par des autorités de certification (dites CA, pour « Certification Authority »). Ce modèle est générateur de coûts importants, rend la révocation difficile, et ne permet pas la production de clés privées à la demande comme c'est le cas avec BIP32. Il est également très largement superflu pour gérer des situations de relations dans lesquelles l'enrôlement des parties est fait par les parties elles-mêmes, en connaissance de cause.

Les identités auto-générées de type blockchain permettent a contrario à chacun de signer numériquement de façon certaine :

- La publication de l'intention d'utiliser une identité
- La publication d'une révocation
- La confirmation ou validation d'une autre identité (pour attester que celui qui la détient est bien celui qui il prétend être)
- La déclaration d'une identité secondaire de secours (pour révoquer la première en cas de perte)
- La désignation d'une identité ayant procuration de révocation

Lorsqu'une identité numérique générée sous contrôle d'un usager est utilisée dans une première interaction avec une autre identité, les deux parties se connaissent, et peuvent ainsi engager mutuellement leur validation. Ce processus est connu depuis longtemps dans les milieux utilisant les algorithmes de signature/chiffrement PGP (« Pretty Good Privacy ») et GPG (« Gnu Privacy Guard »), dont les utilisateurs sont engagés dans des « parties » de reconnaissance mutuelle en présentiel. Il est facilité dans le cas qui nous intéresse ici.

Publication des identités sociales blockchain. Aujourd'hui, les réseaux sociaux jouent un rôle important dans l'écosystème de l'authentification, car souvent on nous demande de prouver l'accès à un compte pour accéder à un autre compte : « connectez-vous à Google avec votre compte Facebook », « connectez-vous à ce service via France Connect ou OpenID Connect ». Dans certains cas, comme par exemple en Afrique, le compte Facebook peut être utilisé comme preuve d'identité.

Ces réseaux peuvent être utilisés aussi pour publier une clé publique que l'on utilise pour s'identifier/authentifier[6]. Un des avantages de ce procédé est que les moteurs de recherche ont dans certains cas accès à cette information.

Les blockchains peuvent également être utilisées de diverses manières pour produire un registre inviolable et publiquement auditable (c'est-à-dire vérifiable par tous) des statuts d'identités (publié, révoqué, validé par…). C'est possible notamment avec la sécurité apportée par une blockchain publique, par une sidechain sur Bitcoin, ou par un smart contract sur Ethereum.

Identité auto souveraine et blockchain. A ce qui précède, on peut comprendre que le modèle d'identité apporté par les blockchains permet le stade ultime de l'identité dite 'auto souveraine' dans le contexte de la RGPD : l'usager ne communique aucune information personnelle pour réaliser une transaction.

Sur cette base, il est possible de donner un contrôle total aux usagers d'un service sur les informations personnelles qu'ils acceptent de fournir.

Identité souveraine et preuves « zero knowledge ». On peut même aller plus loin en utilisant des algorithmes comme ZK-Snark (https://media.consensys.net/introduction-to-zksnarks-with-examples-3283b554fc3b) utilisés notamment par la cybermonnaie ZCash (https://z.cash/technology/zksnarks). Ces algorithmes permettent par exemple de prouver que l'on a plus de 18 ans sans révéler son âge réel.

Combinées à l'utilisation d'identité numérique fondée sur les adresses de paiement des blockchains, on voit que les preuves ZK-Snark fournissent sur étagère la réponse aux exigences de l'identité auto souveraine.

MATURITE

La première blockchain a fait son apparition en 2008 comme technologie sous-jacente de la cybermonnaie Bitcoin. Elle aurait été développée par Satoshi Nakamoto, personnage dont l'identité reste inconnue.

Depuis, la technologie blockchain a aussi été envisagée et prototypée pour de très nombreux cas d'usage non monétaires, comme le partage de production locale

[6] Par exemple : https://twitter.com/laurenthenocque/status/602215777626890241

d'énergie, la notarisation de cadastre numérisé (en Afrique, dans des pays n'en disposant pas), la traçabilité de certains produits et aliments, les smart contracts, la dématérialisation de documents (actes notariaux, preuves de propriété), le vote électronique, le transfert de propriété virtuelle, la dématérialisation de transactions financières avec de la monnaie « traditionnelle », la création d'actifs collectionnables (les crypto chats), la création d'entités autonomes décentralisées (les DAO), etc.

DEPLOIEMENTS /UTILISATION SUR LE TERRAIN

Le problème natif de l'utilisation de ces nouveaux moyens d'authentification est la conservation des clés privées par leurs détenteurs. En un sens, ce problème diffère peu de celui adressé par les cartes de paiement à microprocesseur : le dispositif de signature est embarqué dans un élément de sécurité qui préserve des secrets impossibles à exporter. Il y a plusieurs stratégies possibles de génération de ces secrets dans le monde des cybermonnaies :

- La clé privée, ou la racine d'un arbre de dérivation de clés de type BIP32 est générée sur la base d'un secret connu de l'usager seul (éventuellement par dérivation d'un mot de passe) comme cela est possible par exemple sur http://bip32.org/#bip32,
- La clé privée (ou racine comme ci-dessus) est générée à partir d'un nombre aléatoire de bonne qualité dans un dispositif physique (clé Ledger, Fido, Trezor, Archos, HSM…)

Concernant la conservation de ces secrets, plusieurs possibilités existent à nouveau :

- Préservation par le dispositif (wallet) physique (cf. liste ci-dessus), avec ou non possibilité d'export d'une clé maître de sécurité au format BIP39[7]
- Préservation par un wallet logiciel chiffré par un mot de passe sous le contrôle de l'usager (typique des sites de gestion de cybermonnaies comme Blockchain.com[8]

Concernant la dérivation des adresses de paiement (outils d'identification dans notre cas), une variété d'options existe également : BIP32 comme évoqué plus haut, mais aussi BIP44, BIP49, BIP84, BIP141… Cette génération possède une propriété fondamentale : il est possible de prouver qu'une signature est valide et produite par une clé privée dérivée d'une clé publique maître connue. De la sorte, il est possible de prouver à la fois sa capacité à signer et l'appartenance à un schéma de dérivation de clé. Par exemple, il est possible de fournir des identités numériques à un groupe de personne identifié par cette clé publique maître.

[7] https://iancoleman.io/bip39/
[8] https://www.blockchain.com

Lien avec l'identité régalienne. L'Etat est le premier fournisseur d'identité, en mesure de fournir un certain nombre de garanties sur le patronyme, la date de naissance, diverses propriétés biométriques (taille, sexe, couleur des yeux, des cheveux, empreintes digitales) telles que présentées sur une carte d'identité ou stockées dans un élément sécurisé sur le passeport.

Chaque français se voit associer un numéro d'identification unique à vie (appelé numéro INSEE). Rien n'empêcherait que ce numéro fournisse l'index d'une clé publique de référence dans un arbre de dérivation BIP32, permettant ainsi à la personne de disposer d'un espace illimité de moyens de preuve d'identité à usage unique et validés par le gouvernement, tout en préservant toutes les libertés possibles de révocation en cas de perte.

De plus comme indiqué plus haut, l'utilisation d'algorithmes de preuve « zero knowledge » (ZK-Snark) associés aux objets physiques CNI/Passeport permettrait par exemple d'attester que l'on est majeur sans révéler son âge ou que l'on habite en France sans révéler dans quelle ville.

D'autres organismes sont pourvoyeurs d'autres ensembles de confirmation : par exemple, les factures d'eau ou d'électricité sont des preuves de domicile secondaire toujours plus à jour que l'adresse figurant sur un passeport. Comme envisagé plus haut, ces services pourraient confirmer la réalité d'une adresse postale attachée à une clé publique d'identification, permettant ainsi à l'usager d'utiliser cette clé lorsqu'il veut apporter cette preuve, et d'utiliser une clé jetable quand ce n'est pas nécessaire.

CONTRAINTES

Une problématique de la blockchain, quelle qu'en soit la technologie sous-jacente, est la **scalabilité**, i.e. la capacité de pouvoir accueillir de plus en plus d'utilisateurs et donc des transactions et des données. Selon une étude effectuée par Systematic[9], en novembre 2016, la taille de la blockchain de bitcoin était 92 GB, alors que ce chiffre a monté à 209 Gb en mars 2019. On considère toutefois aujourd'hui que la taille de la blockchain Bitcoin est dérisoire par rapport aux ressources de stockage utilisées notamment pour conserver des archives intégrales et incrémentales de l'état d'internet[10].

Selon cette même étude, il est mentionné que la blockchain de bitcoin peut atteindre un **débit** maximum de 7 transactions par seconde, ce qui est encore loin des capacités transactionnelles d'autres réseaux qui atteignent 2.000 transactions par seconde avec des pics à 10.000 transactions par seconde (des réseaux comme VISA peuvent même atteindre des pics de 20.000 transactions par seconde). Les développements récents de sidechains à très haut débit sur Bitcoin permettent

[9] https://systematic-paris-region.org/wp-content/uploads/2017/07/Systematic-LB-Blockchain-HD.pdf
[10] The wayback machine : http://archive.org/web/

aujourd'hui d'écarter ces difficultés. Le réseau lightning[11] qui permet d'établir des canaux de paiement extrêmement rapides est actuellement en déploiement. Le réseau de smart contracts RSK (Rootistock)[12] également.

Ces transactions contiennent aussi des opérations de vérification, de validation et de cryptographie qui peuvent être gourmandes en **consommation d'électricité**. La preuve de travail utilisée par les blockchains publiques (Bitcoin et Ethereum) est la seule option connue dans le contexte d'une blockchain publique permettant une preuve définitivement inviolable de l'état d'un registre. Le coût électrique du minage est donc à ce jour une nécessité incontournable. On doit noter également que le coût énergétique total des grands réseaux de paiement et de réconciliation (Visa, Swift) est colossal.

Même si certains aspects théoriques de la cyber sécurité des blockchains restent à étudier, la communauté des experts en cybermonnaies, ainsi que les acteurs industriels qui l'utilisent, considèrent que le bug-bounty massif attaché à Bitcoin (plus de 100 Milliards d'euros de valorisation) garantit que les algorithmes sous-jacents (sha256, ripemd160, la courbe secp256k1 notamment) sont à ce jour inattaqués, et que toute fragilité annoncée sera signalée et corrigée extrêmement vite. En revanche, la cyber sécurité des blockchains privées, de consortium ou permissionnées constitue un enjeu considérable, car elle reste extrêmement fragile, et repose sur de très nombreuses problématiques habituelles de gestion de systèmes informatiques.

Comme ceci a été discuté précédemment, la définition d'un consensus joue un rôle très important au déroulement et la **gouvernance** d'une blockchain. Qui a accès à la blockchain, qui définit les modalités d'un ajout sur la chaine, comment décider d'une évolution du protocole ? Ce choix est une question plutôt stratégique. La blockchain peut être publique (ouverte à tous) ou privée (avec un nombre limité de participants et, éventuellement mais non nécessairement, l'existence d'une forme d'autorité centralisée). La blockchain sert comme support d'enregistrement sécurisé des transactions et la question de la vérification de l'identité électronique des biens ou des personnes se pose. L'interfaçage entre le monde « numérique » et le monde « traditionnel/réel » est alors au cœur de ces technologies. Aujourd'hui, des efforts importants sont faits pour la standardisation des différents aspects de cette technologie (voir aussi le paragraphe lié à la normalisation).

NORMALISATION

Les efforts principaux connus à ce jour :

[11] Fast Channel payments on Bitcoin https://en.wikipedia.org/wiki/Lightning_Network
[12] Rootstock Smart Contracts on Bitcoin https://www.rsk.co/

- ISO via le comité technique ISO/TC307 dédié aux blockchains et aux DLT (Distributed Ledger Technologies) : https://www.iso.org/committee/6266604.html
  Au sein de ce comité, les groupes de travail suivants ont été constitués :
  - WG1 : Terminology
  - WG2 : Security, Privacy and Identity
  - SG1 : Reference architecture, taxonomy and ontology
  - SG2 : Use cases
  - SG3 : Security and privacy
  - SG4 : Identity
  - SG5 : Smart contracts
  - SG6 : Governance of blockchain and distributed ledger technology systems
  - SG7 : Interoperability of blockchain and distributed ledger technology systems
- NIST avec la publication du « Blockchain technology overview » : https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

LICENCES/BREVETS

La technologie blockchain a été initialement présentée dans un whitepaper[13]. Le parti pris de Satoshi Nakamoto a été de publier les codes sources du protocole bitcoin sous une licence open source MIT. Cette licence de logiciel, dont le code source est ouvert et basé sur des logiciels libres, permet d'utiliser, copier, modifier, fusionner, publier, distribuer, sous-licencier et/ou vendre des copies du logiciel sous réserve d'ajouter une notice de copyright dans toutes les copies ou parties substantielles du logiciel. Dans le cas de modification ou distribution du logiciel, elle ne contraint pas à conserver la même licence et des termes analogues à cette licence.

La blockchain privée *Hyperledger,* une des plus utilisées à nos jours, est distribuée avec une licence Apache 2.0. Cette licence est un peu plus restrictive en obligeant les « contributeurs » à donner leurs brevets en licence dès lors qu'une de leurs innovations incorporerait le code source de cette blockchain. En d'autres termes, elle conditionne la licence à une renonciation à toute action en contrefaçon dont la blockchain en cause serait l'objet.

La blockchain publique *Ethereum* utilise une licence GNU/GPL2 qui contraint tous les logiciels sous les termes GNU/GPL à être distribués sous le même régime GNU/GPL.

[13] http://satoshinakamoto.me/bitcoin-draft.pdf

Dans ces conditions, il n'est pas surprenant de constater un grand nombre de dépôts de brevet relatifs à la blockchain.

La Figure 1 montre le top 10 des entreprises ayant déposées des brevets relatifs à cette technologie, ainsi que le nombre de brevets déposés en février 2018[14].

1	BANK OF AMERICA	45
2	EITC HOLDINGS	42
3	COINPLUG	39
4	ALIBABA	36
5	IBM	34
6	NCHAIN HOLDINGS	33
7	BUBI TECHNOLOGY	30
8	MASTERCARD INTERNATIONAL	21
9	HANGZHOU FUZAMEI TECHNOLOGY	19
10	HANGZHOU YUNPHANT NETWORK TECHNOLOGY	18

Figure 1 : Top 10 des entreprises ayant déposé des brevets

ACTEURS PROMOUVANT CETTE TECHNOLOGIE

Ces dernières années, plusieurs acteurs se sont positionnés sur ce secteur, et un grand nombre d'entreprises « traditionnelles » essaie de capter une part de ce marché. Parmi ces dernières, une des plus importantes est IBM qui dispose aussi d'un grand nombre des brevets (voir Figure 1).

La France suit cette vague avec un nombre important d'entreprises qui ont vu le jour ces dernières années. La Figure 2 présente un panorama des entreprises françaises actives dans ce domaine catégorisé selon leur domaine d'application.

[14] Source : https://bitcoinpatentreport.com/2018/02/04/the-top-10-patent-list/

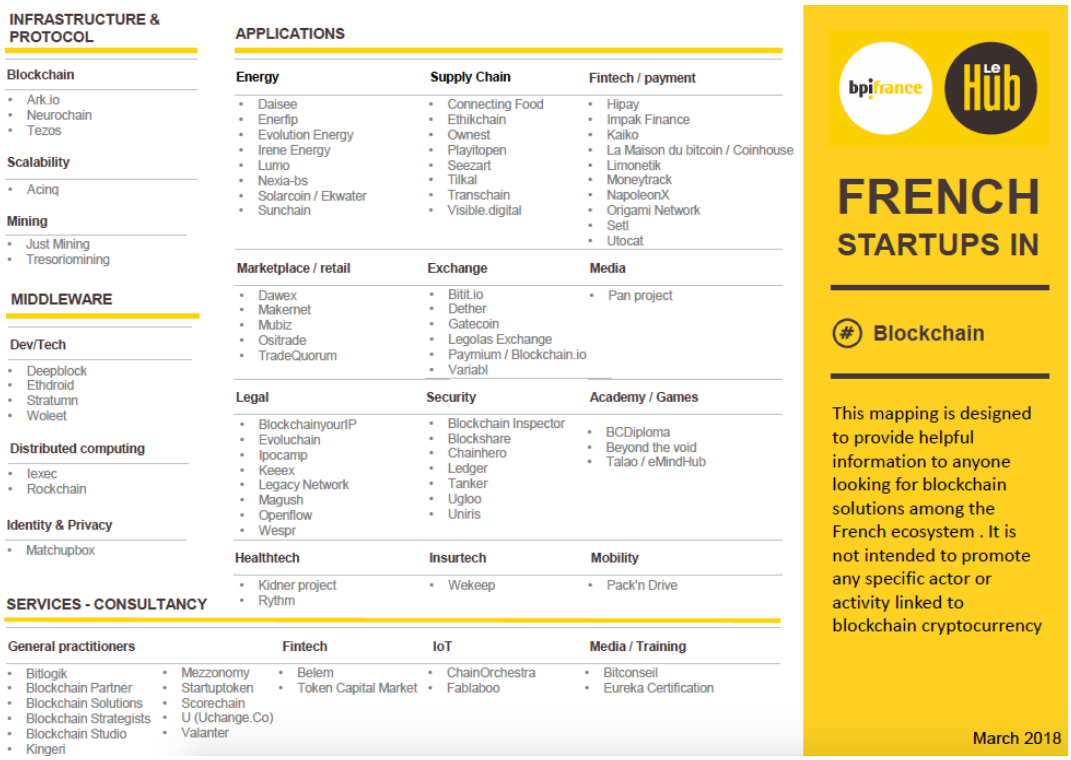


Figure 2: Startups françaises[15]

En complément de ces entreprises, des consortiums ont aussi été constitués afin de concentrer l'effort autour de ces activités, et identifier les besoins de chaque secteur traditionnel. Dans cette catégorie, on trouve par exemple l'Energy Web Foundation dans le domaine de l'énergie, ou encore le labChain (initiative français) et le R3 CEV dans le domaine financier avec une grande participation des acteurs français dans ces consortiums internationaux.

La forte attractivité de cette nouvelle technologie a conduit le magazine Fortune à établir pour la première fois un classement des 40 plus grandes stars (de moins de 40 ans) du secteur blockchain et fintech en 2018[16].

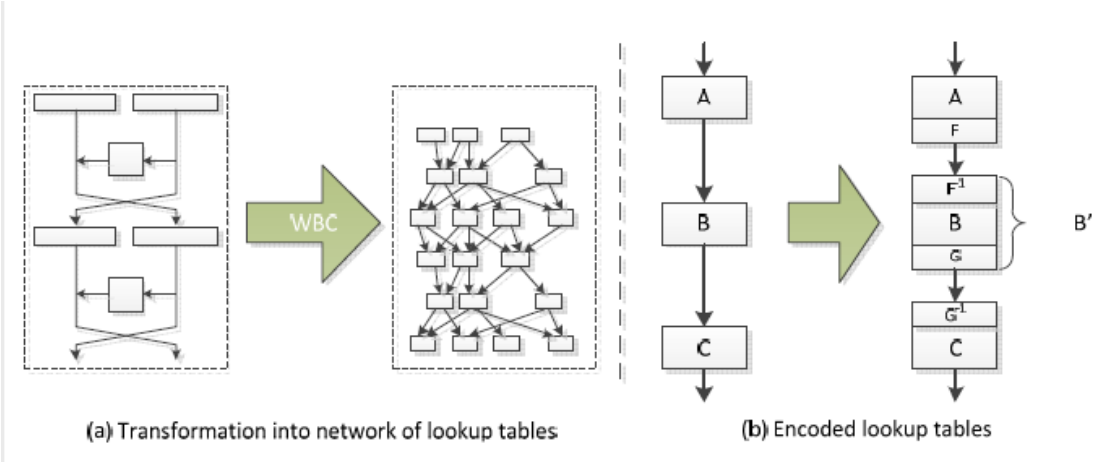
[15] Source : https://blog.lehub.bpifrance.fr/decouvrez-lecosysteme-blockchain-francais/
[16] https://cryptonaute.fr/classement-40-entrepreneurs-blockchain-fintech-2018/

Cryptographie en boîte blanche

La cryptographie en boîte blanche, ou WBC (White Box Cryptography) en anglais, était à l'origine utilisée pour le DRM (Digital Right Management – gestion de droit numérique), mais est devenue très populaire en 2015 lorsque Visa et Mastercard ont choisi de déployer des applications de paiement mobile (technologie HCE-Host Card Emulation).

DESCRIPTION DE LA TECHNOLOGIE

Les premiers articles académiques sur la WBC ont été publiés en 2002 par Chow *et al.* ([ChowDES] et [ChowAES]). Ces articles décrivent une implémentation théorique protégée dans un modèle boîte blanche du système de chiffrement par bloc DES puis de l'AES. Voir ci-dessous un extrait de [Misc2012] décrivant le principe de la WBC par Chow *et al.* :



L'objectif de la WBC est de cacher la clef symétrique (du DES, de l'AES…) dans le code ou dans les données du mécanisme de chiffrement par bloc (voire dans le code et les données), et de garantir la sécurité de cette clef lors de l'exécution. Cela s'applique aussi aux algorithmes à clef publique (par exemple le RSA).

Il faut toutefois noter que d'autres protections logicielles sont nécessaires pour la sécurité globale de la solution, comme détaillée dans le Rapport Technique TR 103 642 et l'ETSI (voir ci-dessous la partie Normalisation).

On distingue la WBC statique (la clef secrète est cachée dans le code) de la WBC dynamique (la clef est passée en paramètre, dans un format protégé, à chaque appel de la fonction). La WBC dynamique permet de distribuer le même code (ou la même application) à tout le monde et ne personnaliser que la clef, ce qui est un avantage pour le déploiement.

Dans le modèle d'attaque en boîte blanche, l'attaquant a un contrôle complet sur la plateforme d'exécution (appels CPU, registres mémoire…) ; il a également accès et peut modifier le code binaire. Ce modèle est parfaitement adapté aux implémentations sur mobile, où les applications (par exemple une application de paiement) s'exécutent dans un environnement potentiellement compromis.

MATURITE

Aujourd'hui, la plupart des solutions théoriques de WBC publiées sont cassées, et c'est là toute la difficulté : comment convaincre de l'efficacité de la WBC (et plus généralement des protections logicielles), comment démontrer qu'elle constitue une alternative « sûre » lorsque la sécurité fournie au niveau hardware (e.g. SE-Secure Element, TEE-Trusted Execution Environment ou TPM-Trusted Platform Module) ne peut pas être utilisée.

Des Challenges sont organisés pour confronter les implémentations white box aux aptitudes des hackers. On peut citer le Challenge de CHES (https://whibox-contest.github.io/2017/, https://whibox-contest.github.io/2019/), qui a pour objectif de recevoir des implémentations WBC AES-128 (supposées résister à une extraction de la clef), et de proposer ces implémentations aux attaquants inscrits (anonymement ou pas) pour qu'ils extraient la clef de chiffrement enfouie dans le code.

L'analyse d'un code logiciel protégé par la WBC est au confluent des techniques de reverse (qui se développent depuis une quarantaine d'années), des attaques hardware (qui sont connues depuis une vingtaine d'années, et facilement transposables au logiciel) et des attaques cryptographiques. Il existe notamment de nombreux outils en open-source, des démonstrations d'attaques et des publications, qui « facilitent » le travail des attaquants.

Enfin, on peut noter que dans le domaine de la cryptographie en boîte blanche, il existe une différence significative entre les propriétés de sécurité considérées sur le plan théorique et les propriétés de sécurité attendues dans un contexte de produit industriel. En théorie, les spécifications sont connues de l'attaquant, qui cherche par exemple à retrouver la clef. En pratique, dans un cas industriel, les spécifications ne sont pas disponibles, afin de compliquer et retarder le travail de l'attaquant.

CONTRAINTES

Les contraintes induites par l'utilisation de la WBC sont principalement le besoin de pouvoir changer régulièrement les clefs et de pouvoir mettre à jour sur le terrain les implémentations logicielles protégées en WBC.

Une autre contrainte importante dans le cas de la WBC est le fait qu'il n'y ait pas de source d'entropie locale fiable, alors même que les générateurs aléatoires sont

essentiels en cryptographie, et largement utilisés dans les contre-mesures classiques permettant de protéger les implémentations cryptographiques.

Les contraintes classiques de performance et de taille sont aussi pertinentes dans le contexte WBC.

Dans un contexte plus général de sécurisation logicielle (englobant la WBC), une contrainte importante est le coût d'une solution WBC solide pour les algorithmes standardisés ; en effet, remplacer un design cassé n'est pas immédiat, et justifie la nécessité de la diversification du logiciel pour circonscrire l'impact d'une attaque réussie. Une autre contrainte est le déploiement de logiciel via un App Store où il faut convaincre que le code protégé n'est pas un malware et également prendre le risque du passage à l'échelle d'une attaque.

NORMALISATION

ETSI TC CYBER

https://portal.etsi.org/tb.aspx?tbid=824&SubTB=824,856

L'ETSI a publié un document traitant des techniques de protection logicielles, ETSI Technical Report (TR) 103 642 « *CYBER; Security techniques for protecting software in a white box model*", Version 1.1.1, Octobre 2018

https://www.etsi.org/deliver/etsi_tr/103600_103699/103642/01.01.01_60/tr_103642v010101p.pdf

Ce document liste les techniques utilisées pour protéger les implémentations logicielles. Cette liste inclut la cryptographie en boîte blanche (WBC), l'obfuscation de code ainsi que d'autres techniques, notées anti-xxx et incluant les mécanismes d'anti-tampering, anti-reverse, anti-debug, anti-clonage, etc… Le document classe également les menaces et indique comment s'en protéger en utilisant les différentes techniques. Le cas des attaques sur les implémentations en boîte blanche est traité à part.

L'ETSI a également publié un document traitant des méthodes des « *External* encoding » pour l'AES, mais aussi l'applicabilité aux autres algorithmes de chiffrement par bloc. Il s'agit du ETSI Technical Specification (TS) 103 718 « CYBER ; *External encodings for the Advanced Encryption Standard* », Version 1.1.1, Octobre 2020.

https://www.etsi.org/deliver/etsi_ts/103700_103799/103718/01.01.01_60/ts_103718v010101p.pdf

FIDO Alliance

https://fidoalliance.org/

FIDO Alliance développe un programme de certification pour les solutions d'authentification basées sur du software et protégées par des méthodes purement software (incluant les mécanismes listés dans le document ETSI TR 103 642), identifié par la terminologie L1+.

Ce programme de certification, inclut une analyse par un laboratoire externe accrédité par FIDO Alliance et des tests de pénétration, selon une nouvelle méthode d'évaluation inspirée des Critères Communs.

Ce programme finalisé et sera publié courant Q3 2021, avec la prochaine version des spécification sécuritaires (version 1.5).

ISO/IEC JTC1/SC27/WG3

https://www.iso.org/standard/78890.html

L'ISO/IEC prépare un guide pour le test et l'évaluation de la cryptographie en boîte blanche, sous la forme d'un Technical Report. TR 24485.2 « *Information technology – Security techniques – Security properties, test and evaluation guidance for white box cryptography* ».

Le document décrit les propriétés de sécurité attendues pour la WBC (secret et intégrité de la clef, diversification, difficulté de lifter ou reverser le code), donne des guides pour des tests ainsi que pour une évaluation (incluant la description des attaques à considérer, comme l'analyse des tables, les side-channels ou l'injection de faute).

CAS D'USAGES IDENTIFIES

Cette technologie a d'abord été utilisée dans le cadre du DRM (Digital Right Management). Il faut noter que les schémas de DRM peuvent utiliser, en plus des techniques de protection software comme la WBC ou l'obfuscation, des techniques de sécurité par l'obscurité (incluant notamment l'utilisation d'algorithmes non standardisés et/ou propriétaires), ce qui n'est pas possible dans des applications de type bancaire où tout est normalisé.

La technologie WBC s'est ensuite étendue à tous les cas d'usage impliquant des dispositifs (smartphone, tablette, ordinateur) où il n'est pas possible d'utiliser les éléments de sécurité hardware présents (pour des raisons d'accessibilité, notamment de disponibilité d'API, pour des raisons de licence, ou encore lorsqu'on ne sait pas sur quel type de dispositif l'application va être chargée).

Ces cas d'usages sont notamment le paiement dans le nuage (et la technologie HCE), ou encore le domaine de l'automobile.

Ces cas d'usage sont décrits en détail dans le document ETSI TR 103 642.

LICENCES ET BREVETS

Une simple recherche « patents on whitebox crypto » sur Google fait ressortir des brevets détenus par des industriels tels que Irdeto, Philips Electronics, NXP B.V, Apple, Cloakware, Orange, Gemalto, etc., ainsi que par des universités telles que Institute of Information Engineering http://www.iie.ac.cn/ ou Guilin University of Electronic Technology https://www.gliet.edu.cn/.

ACTEURS PROMOUVANT CETTE TECHNOLOGIE

Voilà une liste non exhaustive d'acteurs par ordre alphabétique :

- ✓ Apple
- ✓ Arxan
- ✓ CryptoExperts
- ✓ Google
- ✓ Idemia
- ✓ Inside Secure
- ✓ Irdeto
- ✓ Microsoft
- ✓ Nagra
- ✓ Promon
- ✓ Secure-IC
- ✓ Sony
- ✓ Thales
- ✓ Trustonic
- ✓ Whitecryption

On peut inclure à cette liste les sociétés fournissant des outils d'analyse pour la WBC :

- ✓ Eshard
- ✓ Quarkslab
- ✓ Riscure

Conclusion

Le sujet de la cryptographie en boîte blanche est un sujet essentiel pour la sécurisation des clefs cryptographiques dans un contexte d'implémentation logicielle. Plusieurs industriels proposent déjà des solutions. Cependant, on remarque que les propriétés de sécurité considérées dans les publications théoriques de WBC ne correspondent pas aux propriétés de sécurité attendues dans les produits et solutions logicielles faisant intervenir la WBC.

La WBC est un élément important de la sécurisation logicielle des mécanismes cryptographiques. Cependant, il est important de la combiner à d'autres techniques de sécurisation logicielle. En effet, protéger la clef de chiffrement ne suffit pas. Un attaquant pourrait par exemple copier la WBC afin de pouvoir réutiliser la fonction cryptographique sans avoir connaissance de la clef, et chiffrer/déchiffrer. Il est donc nécessaire d'utiliser d'autres techniques de protection (comme l'obfuscation) afin de fournir une protection par couches, plus difficile à casser. Ces différentes techniques sont décrites dans le TR 103 642 de l'ETSI.

Bibliographie

[ChowDES] Stanley Chow, Philip A. Eisen, Harold Johnson, and Paul C. van Oorschot. "A white-box DES implementation for DRM applications", Proceedings of the ACM Workshop on Security and Privacy in Digital Rights Management, volume 2696, LNCS, 2002.

[ChowAES] Stanley Chow, Philip A. Eisen, Harold Johnson, and Paul C. van Oorschot. « White-Box

Cryptography and an AES Implementation », Proceedings of the 9th International Workshop on Selected Areas in Cryptography, volume 2595, LNCS, 2002.

[MISC2012] Brecht Wyseur, "White-box cryptography: hiding keys in software", Misc, 2012.

Cryptographie « Zero Knowledge »

DESCRIPTION DE LA TECHNOLOGIE

Ainsi que le décrit Wikipedia[17], les méthodes cryptographiques « **Zero Knowledge** » s'appuient sur « un protocole sécurisé dans lequel une entité nommée « fournisseur de preuve », prouve mathématiquement à une autre entité, le « vérificateur », qu'une proposition est vraie sans toutefois révéler d'autres informations que la véracité de la proposition ». On authentifie donc une personne ou une action sans dévoiler le processus ni les données d'authentification.

Nous prendrons l'exemple de deux personnes disposant de deux verres identiques : l'un contient de l'eau, l'autre un poison ressemblant à de l'eau.

La technologie met en œuvre 3 échanges (au minimum) :

- Le fournisseur de preuve indique au vérificateur la propriété qu'il peut vérifier : « je peux distinguer l'eau du poison ». Le vérificateur ne peut reconnaitre l'eau du poison mais doit vérifier que l'assertion du 'prouveur' est vraie.
- Le vérificateur mélange alors (ou non) les deux verres et renvoie un défi au prouveur : « la position des deux verres a-t-elle changé ? ».
- Le prouveur retourne sa réponse au vérificateur : s'il ne dispose pas de la propriété annoncée, il a 50% de risques de retourner une réponse erronée. Ce risque augmente à chaque boucle du protocole.

Après 10 échanges « défi / réponse » positifs, la probabilité pour que le prouveur dispose vraiment de la propriété annoncée s'élève à 99.9%[18].

Une méthode d'authentification (ou de vérification de preuve) peut être :

- Interactive : la validation est basée sur une estimation statistique de la qualité de la preuve, suite à de nombreux échanges défi/réponse entre client (prouveur) et serveur (vérificateur)
- Non-interactive : le protocole n'exige qu'un seul échange client vers serveur, limitant ainsi les contraintes techniques (voir plus bas)

[17] https://fr.wikipedia.org/wiki/Preuve_%C3%A0_divulgation_nulle_de_connaissance
[18] Au bout de N tours, la probabilité = $1 - 0.5^N$ *100%

Un protocole cryptographique « zero knowledge » doit satisfaire 3 propriétés essentielles :

- La consistance : le vérificateur doit accepter toute preuve fournie conformément au protocole et ne peut « présupposer » que celle-ci a été « devinée ».
- La robustesse : une preuve fausse doit interrompre le processus de validation sans ambiguïté.
- L'absence de nécessité de preuve ('zero knowledge') : seule la véracité de l'assertion est vérifiée, le vérificateur ne reçoit aucune information supplémentaire qu'il ne connaisse à l'énoncé de l'assertion.

MATURITE

Les travaux initiaux, ou plutôt leur première formulation structurée, sont dus à Shafi Goldwasser, Silvio Micali et Charles Rackoff, en 1985. Depuis cette date, de nombreux algorithmes répondant à cette définition initiale ont été développés pour s'adapter à différents cas d'usage.

Il est à noter que, sur un plan purement mathématique, les protocoles dits « ZKP » (Zero Knowledge Proof) s'appuient sur des méthodes de chiffrement standard : AES-256, RSA-2048 ou -4096, ce qui leur permet d'être mis en œuvre sur de nombreux supports.

Il existe aujourd'hui des implémentations open source sous forme de librairies javascript, C++, ou PKCS #5 (RFC 2898).

DEPLOIEMENTS/UTILISATION SUR LE TERRAIN

Avec l'essor du stockage dans le cloud, à destination des particuliers comme des professionnels, et les craintes grandissantes autour de la confidentialité et l'intégrité des informations confiées aux fournisseurs de stockage, de nombreuses solutions commerciales intègrent désormais une technologie ZKP :

- Stockage cloud et partage de fichiers : Tresortit[19], StorGrid[20], pCloud[21]
- Gestion d'identité : SailPoint[22]
- Partage de document temps-réel : CryptPad[23]
- Cryptomonnaie / blockchain : Zcash[24]
- Gestionnaire de mots de passe : Keeper[25]

[19] https://tresorit.com/
[20] https://www.storgrid.com/storgrid-launches-zero-knowledge-encryption-2/
[21] https://www.pcloud.com/fr/features/crypto.html
[22] https://www.sailpoint.com/
[23] https://cryptpad.fr/
[24] https://z.cash/fr/technology/zksnarks/

Il faut également noter que cette technologie fait l'objet de quelques initiatives de la part des grands acteurs généralistes que sont Microsoft, avec son offre libre U-Prove[26], qui permet de révéler la présence ou la validité de certains attributs au sein d'un 'token' (élément cryptographique s'apparentant à un certificat) sans en dévoiler la valeur, ou encore d'IBM dont le protocole Identity Mixer poursuit le même but.

Microsoft U-Prove est aujourd'hui supporté par une spécification complète associée à un SDK. Cette technologie a été mise en œuvre partiellement dans le projet européen ABC4Trust. Pour sa part, IBM a placé son projet Idemix en libre accès sur Github[27].

CONTRAINTES

Les protocoles ZKP affichent néanmoins quelques contraintes, notamment un important besoin en ressources de calcul (formules polynomiales complexes) et en mémoire, le chiffrement/déchiffrement étant fait sur le client jouant le rôle de prouveur : le prouveur reçoit la donnée chiffrée après avoir résolu l'authentification et doit la déchiffrer localement, la clé de chiffrement ne quittant ainsi jamais le périmètre du client. Par ailleurs, ces échanges entre client (prouveur) et serveur (vérificateur) sont nombreux, ce qui impose une contrainte supplémentaire sur l'efficacité de la connexion entre les deux entités.

Il est à noter également que la clé privée utilisée pour le chiffrement doit répondre aux exigences de robustesse pour éviter les attaques par force brute.

De plus, dans le cas des applications de stockage de fichiers encryptés dans le cloud, l'accès aux documents à partir d'un autre client impose de gérer le transport de la clé privée via un gestionnaire de mots de passe, comme Keepass, ou une clé USB, ce qui dégrade l'expérience utilisateur. Ce chiffrement peut également empêcher de partager des documents, puisque seule la preuve apportée par le propriétaire du fichier permet de le déchiffrer.

Enfin, certains protocoles ZKP ne sont pas immunisés contre les attaques de type « man-in-the-middle », car si l'assertion initiale est modifiée par un attaquant, celui-ci a les moyens de falsifier la preuve retournée au vérificateur.

---

[25] https://keepersecurity.com/fr_FR/resources/zero-knowledge-for-ultimate-password-security.html
[26] https://www.microsoft.com/en-us/research/project/u-prove/
[27] https://github.com/p2abcengine/p2abcengine/wiki/Concepts-and-features

NORMALISATION

Les protocoles reposent sur un faible nombre de textes normatifs :

- Des normes ISO/IEC
  - ISO/IEC 9798-1:2010 "Information technology -- Security techniques -- Entity authentication -- Part 1: General"
  - ISO/IEC 9798-5:2009 "Information technology -- Security techniques -- Entity authentication -- Part 5: Mechanisms using zero-knowledge techniques"
- Des recommandations du NIST : https://csrc.nist.gov/groups/computer-security-division/cryptographic-technology

CAS D'USAGE IDENTIFIES

Comme vu plus haut, l'application principale de la technologie Zero Knowledge Proof est l'authentification et la garantie d'un accès à des ressources encryptées sans partage des informations de chiffrement.

Cette caractéristique a permis le développement de quelques offres commerciales : stockage en nuage, cryptomonnaies, mais peut aussi être utilisée pour protéger la sécurité de toute information sensible : données financières, données de santé, données industrielles.

Sa mise en œuvre est plutôt adaptée à la protection de données statiques ('*at rest*') plutôt que celle de réseaux de communication.

LICENCES ET BREVETS

De nombreux brevets couvrent cette technologie, en majorité déposés par des sociétés privées opérant des solutions de stockage (classique ou blockchain).

Une recherche rapide via Google Scholar retourne plus de 8800 résultats depuis le 01.01.2017.

ACTEURS PROMOUVANT CETTE TECHNOLOGIE

Ainsi que décrit plus haut, les principaux acteurs utilisant les protocoles ZKP sont principalement des fournisseurs de solutions de stockage ou des fournisseurs de briques technologiques (blockchain notamment, comme QEDit[28] ou la banque ING).

[28] https://qed-it.com/

Cryptographie à seuil

DESCRIPTION DE LA TECHNOLOGIE

Wikipedia donne une très bonne définition de cette technologie : « Un cryptosystème à seuil est, en cryptographie, un cryptosystème tel que le déchiffrement d'un message nécessite la coopération de plusieurs entités ».

Un message est chiffré à l'aide d'une clé publique dont la clé privée correspondante est un secret réparti entre différents participants. En notant S le seuil du cryptosystème et N le nombre d'acteurs entre lesquels le secret est réparti, on ne peut déchiffrer un message que si au moins S participants sur les N coopèrent, et ce *sans reconstruire la clé*.

De manière analogue, on peut concevoir des signatures numériques à seuil : la coopération de S signataires serait alors nécessaire pour délivrer une signature (ou un certificat).

Ainsi, les cryptosystèmes à seuil peuvent être utilisés pour simuler l'existence d'un tiers de confiance par un calcul distribué.

En effet, dans les transactions électroniques, quelle que soit leur nature, il est difficile d'établir un niveau de confiance suffisant avec un serveur unique, qui peut être attaqué et compromettre ainsi tous les secrets qu'il manipule ; il est statistiquement plus sûr de confier ces secrets à un ensemble de serveurs, dont on suppose que la majorité ne sera pas attaquée simultanément ou résistera à l'attaque.

Il est à noter que les schémas de chiffrement sous-jacents peuvent être des schémas classiques, adaptés pour intégrer la notion de seuil, sans diminuer leur niveau de sécurité : ex. le chiffrement RSA ou certains schémas de signature numérique, comme la signature de Schnorr[29], qui repose d'ailleurs sur la technologie ZKP.

Dans le même esprit que la cryptographie à seuil, la cryptographie multi-parties, dont l'étude débuta dans les années 70, repose sur des mécanismes de partage d'une valeur chiffrée en plusieurs fragments, permettant sa distribution et sa reconstruction sécurisées. Le but est de permettre à de multiples entités de détenir une valeur secrète et de participer au calcul du résultat d'une fonction sans dévoiler cette valeur. Un exemple classique est représenté par la situation suivante : 3 participants veulent connaitre le plus important de leurs salaires respectifs (le résultat du calcul) sans dévoiler ces salaires (les valeurs secrètes).

[29] https://fr.wikipedia.org/wiki/Protocole_d%27authentification_de_Schnorr

La cryptographie multi-parties (*Multi-Party Computation*, MPC) doit présenter 2 propriétés de base :

- Le masquage des valeurs secrètes utilisées en entrée : aucune valeur ne doit pouvoir être déduite de l'examen du résultat du calcul (sortie).
- La protection contre la collusion : aucun sous-ensemble des parties en entrée ne peut manipuler le résultat du calcul. La technologie doit permettre soit un calcul correct avec un sous-ensemble restreint de valeurs correctes, soit le signalement explicite d'une impossibilité de calcul.

Elle souffre d'un problème d'efficacité (temps de calcul, messages échangés entre les entités, occupation réseau) lorsque le nombre de participants est élevé : vote électronique, enchères, paiement…

MATURITE

Les premiers travaux sur la cryptographie à seuil identifiés sont l'œuvre d'Yvo G. Desmedt, Yair Frankel[30], en 1989. Ils seront complétés par ceux de Amir Herzberg, Stanislaw Jarecki, Hugo Krawczyk, and Moti Yung[31] en 1995.

Pour la cryptographie multi-parties, nous pouvons citer :

- The Security of Practical Two-Party RSA Signature Schemes. Mihir Bellare, Ravi S. Sandhu, IACR Cryptology ePrint Archive 2001: 60 (2001)
- Generation of Shared RSA Keys by Two Parties. Guillaume Poupard, Jacques Stern: ASIACRYPT 1998.
- Realizing Distributed RSA using Secure Multiparty Computations, Atle Mauland, Master of Science in Communication Technology[32]
- Simple Identity-Based Cryptography with Mediated RSA, Xuhua Ding and Gene Tsudik, CT-RSA 2003
- Fast Secure Two-Party ECDSA Signing, Yehuda Lindell[33]
- Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody, Yehuda Lindell, Ariel Nof and Samuel Ranellucci[34]

On peut donc considérer que cette technologie dispose d'un haut niveau de maturité, assuré par la mise en œuvre d'un seuil au sein de cryptosystèmes très répandus, donc très audités.

---

[30] "Threshold cryptosystems", CRYPTO '89 Proceedings on Advances in cryptology
[31] "Proactive Secret Sharing, or How to Cope with Perpetual Leakage", CRYPTO'95
[32] https://daim.idi.ntnu.no/masteroppgaver/004/4699/masteroppgave.pdf
[33] https://eprint.iacr.org/2017/552.pdf
[34] https://eprint.iacr.org/2018/987.pdf

DEPLOIEMENTS/UTILISATION SUR LE TERRAIN

En 2008, Daniel E. Geer et Moti Yung ne voyaient « pas d'applications sur le marché, tant que la possibilité de fragmenter les clés n'est pas offerte au grand public ». Les applications sont en effet peu développées et se présentent pour la plupart sous la forme de composants logiciels dédiés au chiffrement et à l'authentification. Ces composants sont mis en œuvre dans des applications de type stockage en ligne, PKI ou chiffrement de flux (ex. flux vidéo).

On trouve également des applications dans le domaine IoT où la sécurité globale d'un ensemble d'appareils est assurée de façon distribuée : connexion au hub de communication, signature des commandes pour les actuateurs…

CONTRAINTES

La première contrainte qui apparait est le fait, pour l'entité émettrice du message, de ne pas posséder l'intégralité de la clé privée. Ceci peut nuire au désengagement dans des procédures telles que la « signature de contrat » et annuler les propriétés de non-transférabilité, en cas de défaillance des porteurs de (fragments de) clés au-delà du seuil accepté.

D'autres questions se posent également au sujet de cette technologie :

- Valeur du seuil : quelle fraction du groupe de serveurs peut être attaquée ou corrompue sans dégradation du service qu'ils fournissent (ex. signature ou déchiffrement) ?

- Efficacité : quelles sont les exigences en termes de bande passante, taille de stockage ou puissance de calcul ? Cette question se pose tout particulièrement dans les applications de type IoT (*edge-computing*).

- Modèle de communication : un modèle distribué exige-t-il une communication synchrone, partiellement synchrone, requérant une authentification mutuelle entre toutes les parties ou seulement des liens sécurisés entre les serveurs inclus dans le groupe ?

- Type d'attaques pris en compte : comment doit se comporter un serveur en cas d'attaque ? Peut-il simplement effacer tous les secrets dont il dispose en cas d'attaque, comptant ainsi sur la résilience « statistique » du groupe ?

NORMALISATION

Si elle ne fait l'objet d'aucune normalisation avancée, on peut néanmoins citer le document préliminaire du NIST : NISTIR 8214 "Threshold Schemes for Cryptographic Primitives : Challenges and Opportunities in Standardization and

Validation of Threshold Cryptography"[35], qui définit les bases de cette technologie.

L'ETSI cite également la cryptographie à seuil dans son document SR 019 020[36], pour certains mécanismes de signature répartie entre un serveur (fournisseur de signature) et le terminal de l'utilisateur.

Enfin l'ISO aborde les principes fondamentaux de la cryptographie multi-parties dans le document « ISO/IEC 19592-2:2017 Information technology — Security techniques — Secret sharing — Part 2: Fundamental mechanisms ».

Par ailleurs, ces technologies s'appuient sur des algorithmes classiques : DSS, RSA, ECC, qui sont eux-mêmes bien standardisés.

CAS D'USAGE IDENTIFIES

L'application la plus courante consiste à stocker des secrets à plusieurs emplacements afin d'empêcher l'exploitation du message chiffré et la cryptanalyse ultérieure sur ce message chiffré. Le plus souvent, les secrets « fragmentés » constituent la clé secrète d'une paire de clés de cryptographie à clé publique ou le texte chiffré des hachages de mot de passe stockés.

Historiquement, seules des organisations manipulant des informations très sensibles, telles que les autorités de certification, les forces armées et les gouvernements, utilisaient cette technologie. Cependant, en octobre 2012, après un certain nombre de compromission de mots de passe sur des sites Web publics, RSA Security a annoncé qu'elle publierait un logiciel permettant de rendre la technologie accessible au grand public. L'une des premières applications de ce concept fut réalisée dans les années 1990 par la conception de Certco[37] pour la gestion des transactions électroniques sécurisées.

On voit aussi apparaitre des applications de « signature de groupe » ou « *network Certification Authority* », ou de « partage de fonction », qui permettent par exemple, après un déchiffrement partagé, d'opérer une fonction sensible : reconstruction de clés, distribution de contenu numérique, enchères ou protocole électif.

Les fournisseurs de blockchain font également appel à cette technologie puisque, intrinsèquement, « les cryptosystèmes à seuil peuvent être utilisés pour simuler l'existence d'un tiers de confiance par un calcul distribué. ».

---

[35] https://csrc.nist.gov/publications/detail/nistir/8214/draft
[36] ETSI SR 019 020 V1.1.2 "The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments", https://www.etsi.org/deliver/etsi_sr/019000_019099/019020/01.01.02_60/sr_019020v010102p.pdf
[37] DIN CERTCO, société de certification basée à Berlin, partie du groupe TÜV Rheinland et du Deutsches Institut für Normung e.V.

On peut noter quelques applications remarquables, comme celle décrite récemment pour les "Mobile Ad Hoc Network" (MANET), dans lesquels un ensemble d'équipements de communication ou de nœuds utilise la cryptographie à seuil pour communiquer au sein d'une infrastructure « malléable » (réseaux de type MESH), avec un minimum de ressources.

Erinn Atwater and Urs Hengartner ont également spécifié, en 2016, l'environnement Shatter[38], une infrastructure open source qui s'exécute sur les ordinateurs de bureau, Android et Android Wear, et effectue la distribution des clés au nom de l'utilisateur. Les clés des applications qui délèguent des opérations cryptographiques à Shatter ne sont compromises que lorsqu'un nombre seuil de périphériques est compromis par le même attaquant.

LICENCES ET BREVETS

Une recherche rapide via Google Scholar retourne plus de 12800 résultats depuis le 01.01.2017. La plupart de ces brevets ont été déposés au début des années 2000, les Etats-Unis s'arrogeant la majorité d'entre eux.

ACTEURS PROMOUVANT CETTE TECHNOLOGIE

Comme vu plus haut, les principaux promoteurs de la technologie à seuil sont des fournisseurs de solutions de signature ou de technologie blockchain, à laquelle elle s'adapte particulièrement.

[38] Using Threshold Cryptography to Protect Single Users with Multiple Devices, Erinn Atwater and Urs Hengartner

FIDO

DESCRIPTION DE LA TECHNOLOGIE

Fast Identity Online est une méthode d'authentification destinée au renforcement de l'authentification de l'utilisateur sur les services en ligne, développée par FIDO Alliance (https://fidoalliance.org/). Elle est basée sur une interaction entre :

- Un serveur d'authentification, opéré par le service souhaitant l'authentification (appelé Relying Party-RP dans le vocabulaire FIDO),
- Le navigateur utilisé sur le poste client, qui intègre une couche de communication avec le serveur et
- Un élément sous le contrôle de l'utilisateur ('*Authenticator*'), qui peut être un élément physique sous la forme d'une clé USB, d'un dispositif autonome communicant sans contact avec le poste client ou même d'un téléphone mobile ou un élément logiciel (application mobile).

Un des objectifs de cette spécification est de favoriser l'interopérabilité entre les sites internet mettant en œuvre un contrôle d'accès à un service marchand, administratif, ou applicatif, en introduisant un second facteur d'authentification (2FA) de nature cryptographique, complétant le traditionnel login / mot de passe. FIDO définit également des modes de fonctionnement sans mot de passe et multi-facteurs.

FIDO comprend effectivement plusieurs protocoles : U2F, UAF, FIDO2, tous basés sur la cryptographie à clé publique, mais introduisant divers concepts au fil du temps. La première mouture définit U2F (*Universal 2nd Factor*), qui a originellement été déployé grâce à des clés USB offrant une fonctionnalité de détection de présence de l'utilisateur.

La seconde déclinaison, UAF (*Universal Authentication Framework*), a introduit ensuite la notion d'authentification sans login, évitant à l'utilisateur de procéder à la saisie traditionnelle de son identifiant et de son mot de passe associé lors d'une connexion à un service (page de connexion), pour ne demander qu'une authentification via l'*authenticator*. Bien évidemment, la première connexion nécessite un enregistrement préalable : identifiant + mot de passe + *authenticator* associé.

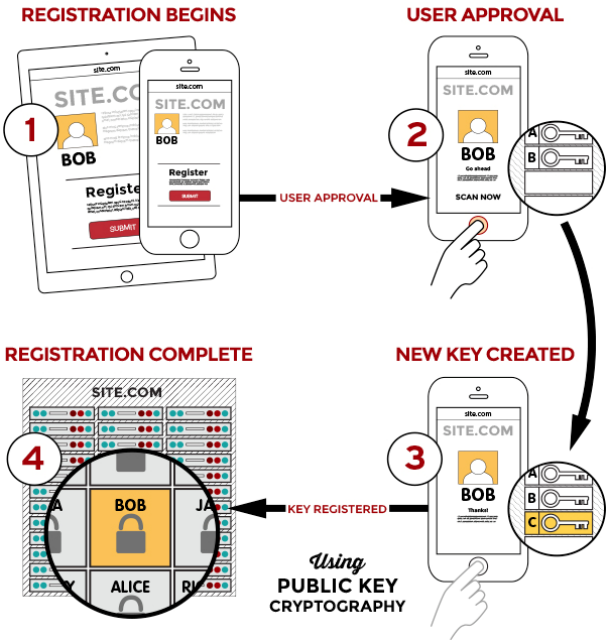
La spécification UAF permet également une sécurité incrémentale : l'authentification renforcée FIDO peut par ailleurs être redemandée lorsque souhaité par le service, pour valider une opération sensible sans redemander le mot de passe. L'utilisateur devra alors s'authentifier à nouveau (code PIN, vérification biométrique…) pour poursuivre la transaction.

FIDO permet aujourd'hui d'opérer l'authentification sur différents canaux de communication : USB, NFC, BLE sont supportés sur les appareils en disposant. Le support BLE a par exemple été nativement inclus dans le système Android, permettant d'utiliser les tokens compatibles sans aucune connexion physique.

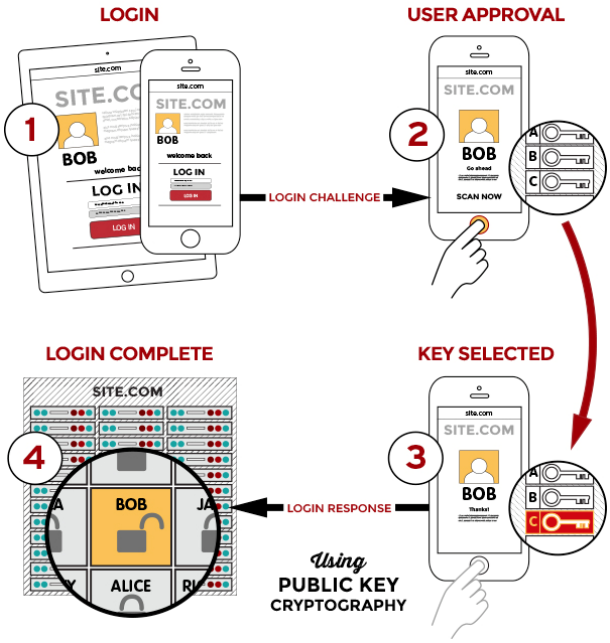
Les variantes UAF et FIDO2 incluent elles le support de la biométrie : empreinte digitale, reconnaissance faciale ou vocale… Une procédure de certification dédiée est d'ailleurs consacrée aux appareils reposant sur la biométrie.

Toutes les versions du protocole mettent en œuvre des processus simples :

- L'enregistrement auprès d'un site compatible FIDO permet de créer la relation initiale entre l'utilisateur, son token FIDO et le service en créant un élément cryptographique unique liant ces 3 entités (paire de clés asymétrique).



- La connexion au service utilise l'élément cryptographique généré lors de l'enrôlement pour valider (second facteur) l'identité de l'utilisateur et recueillir son consentement pour la poursuite de la transaction concernée (ex. la connexion elle-même ou toute autre opération postérieure).



MATURITE

Standard technique imaginé par Paypal, le protocole FIDO a connu plusieurs étapes de développement. L'alliance FIDO fut créée en juillet 2012 par PayPal, Lenovo, Nok Nok Labs, Validity Sensors, Infineon et Agnitio. Ces membres fondateurs, rejoints en 2013 par Google, Yubico et NXP, spécifièrent en avril 2013 le protocole U2F (1er déploiement interne chez Google), qui fut complété par le protocole UAF en décembre 2014. En juin 2015, le support des communications via NFC et BLE est introduit.

Le projet FIDO2 fut mis en œuvre à partir de février 2016, dans l'objectif de standardiser l'utilisation du protocole au sein de tous les navigateurs (FIDO2 2.0 Web API). Cette proposition rencontra l'aval du W3C qui décida d'en inclure le support natif dans l'API Web Authentication[39], favorisant ainsi son adoption.

Depuis mai 2015, l'alliance propose un programme de certification fonctionnel complet, assurant ainsi le respect des spécifications par les différents fournisseurs et l'homogénéité de l'écosystème. Plus récemment, l'alliance a proposé également un programme de certification sécuritaire (https://fidoalliance.org/certification/) selon le niveau de sécurité visé par l'*authenticator* (L1, L2, L3/L3+ sont disponibles, L1+ et L2+ sont en préparation), incluant un programme de certification du composant biométrique utilisé.

Comme indiqué plus haut, les protocoles et leurs évolutions sont maintenus par la FIDO Alliance (https://fidoalliance.org/), qui regroupe de nombreuses entreprises

[39] https://www.w3.org/2016/02/securewebauthwg.html.en

de technologie : Google, Microsoft, Intel, Paypal, Visa, Gemalto, Amazon, Lenovo, Yubiko, etc.

DEPLOIEMENTS/UTILISATION SUR LE TERRAIN

Le poids des acteurs en présence et leur puissance industrielle a bien évidemment favorisé une large adoption du standard. Aujourd'hui, plus de 400 produits sont certifiés par le consortium : tokens physiques, serveurs d'authentification, applications composent un écosystème très riche et dynamique.

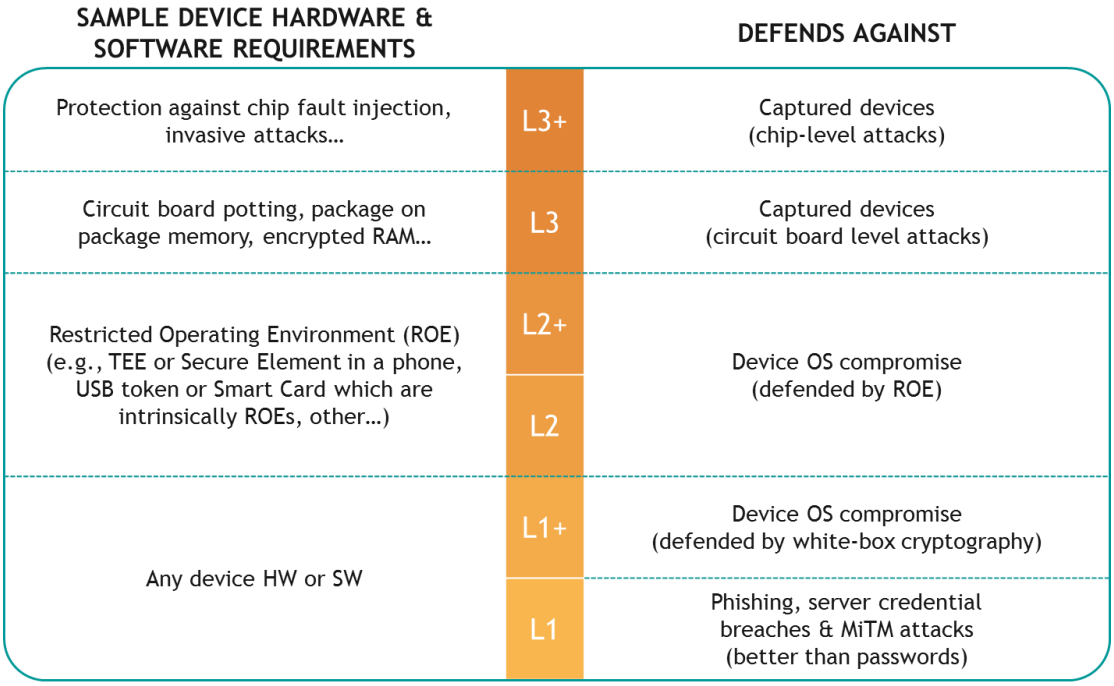
Le standard est applicable dans de nombreux domaines : entreprise, services financiers, santé, administrations, etc. et la simplicité de ses processus favorise l'adoption par les utilisateurs, qui disposent ainsi d'un moyen universel d'accéder à leur service.

Un *authenticator* FIDO supporte la connexion à de multiples services (selon la capacité mémoire de l'élément), tout en garantissant l'étanchéité entre les services : un dispositif enrôlé auprès du service A ne peut être utilisé pour se connecter au service B, même si celui-ci supporte la spécification FIDO.

Le standard est par ailleurs supporté nativement par de nombreux navigateurs internet : Chrome, Firefox, Edge, Opera ainsi que le système Android. Ceci évite une fragmentation certaine, au vu de la diversité des terminaux ciblés.

CONTRAINTES

Les éléments cryptographiques assurant la sécurité de la transaction sont conservés au sein du dispositif physique, qui doit donc répondre à certaines exigences selon le niveau de certification visé (L1 à L3+). Ces différents niveaux de sécurité correspondent aux exigences ci-dessous (extrait d'une présentation FIDO par le Chair du groupe Sécurité) :



Le Secure Element est clairement identifié pour les niveaux L3/L3+, ce qui garantit une sécurité physique de haut niveau. Un Profil de Protection Critères Communs a ainsi été réalisé récemment pour un *authenticator* FIDO U2F par le BSI[40] (BSI-PP-CC-0096-V2-2018), qui vise un niveau de sécurité EAL 4+ et correspond au niveau L3+.

Néanmoins, la spécification impose que les éléments cryptographiques soient générés par l'équipement (ou l'application) lui-même ('*on board generation*'), ce qui interdit de mettre en œuvre un processus de fabrication et de personnalisation industriel, comme nous en connaissons dans l'industrie de la carte à puce, par exemple, où les secrets sont générés et conservés par un système central hautement sécurisé qui permet la gestion complète du cycle de vie de ces secrets.

Nous pouvons également identifier quelques faiblesses dans les différents protocoles :

- Le protocole ne permet pas l'identification de l'utilisateur :
    - L'utilisation d'un dispositif FIDO n'étant pas soumise à un enregistrement auprès d'un tiers de confiance, il n'existe pas de lien vérifiable entre le dispositif et son utilisateur.
    - Avec un élément compatible U2F, l'étape d'authentification peut être simplifiée à l'extrême et consister simplement en l'appui sur un

[40] https://www.bsi.bund.de

bouton mécanique, ne reliant pas l'utilisateur légitime à la transaction validée.

    - Les dispositifs faisant appel à la biométrie disposent d'un avantage dans ce processus, puisque seul l'utilisateur légitime peut déverrouiller l'usage du certificat reconnu par le service.

- En cas de perte ou de vol de l'élément physique, une baisse du niveau de sécurité est inévitable car le voleur peut déclarer la clé perdue sur le service ciblé. Il sera alors redirigé vers une procédure d'authentification dégradée (ex. répondre à des questions), contournable par ingénierie sociale. Ce problème perdure dans la dernière version FIDO2 et est en cours d'étude par l'Alliance (voir à ce sujet la présentation de Yahoo Japan « *account recovery* », https://fidoalliance.org/fido-authentication-account-recovery-framework-at-yahoo-japan/).

- Si l'utilisateur suit le conseil donné par l'Alliance de se munir de deux clés, il devra procéder systématiquement à deux opérations d'enrôlement auprès de tous les services, ce qui est lourd à gérer et sujet à erreur ou oubli.

NORMALISATION

FIDO n'est pas une norme, mais un standard technique largement soutenu et supporté : il a donc force de norme industrielle. La nouvelle version FIDO2 repose d'ailleurs en partie sur une interface spécifiée et standardisée par un autre organisme, le W3C.

Néanmoins, le standard FIDO dispose d'un processus de certification complet, à la fois fonctionnel et sécuritaire, qui assure une diffusion homogène des usages :

- Tests unitaires selon une suite de tests définie par le consortium,

- Tests d'interopérabilité,

- Tests de sécurité,

- Tests spécifiques pour les dispositifs intégrant une reconnaissance biométrique…

Par ailleurs, de nombreux exemples d'implémentation complète sont disponibles librement (Open Source) : serveur, client, et même firmware pour les dispositifs physiques.

FIDO permet également de satisfaire à certaines exigences du RGPD en matérialisant de façon explicite le consentement de l'utilisateur, et répond aux attentes de la règlementation PSD2 en matière de « *strong customer*

authentication ». On peut citer à cet effet les livres blancs publié par FIDO sur ces sujets https://fidoalliance.org/content/white-paper/.

CAS D'USAGE IDENTIFIES

Les cas sont multiples et variés, car tout service requérant une authentification renforcée est candidat à son implémentation.

Nous pouvons citer les domaines suivants :

- Paiement : Bank of America, Paypal, ING
- Télécoms : NTT Docomo, Samsung
- Contrôle d'accès logique : Dropbox
- Commerce : eBay
- Réseaux sociaux : Facebook, GitHub, Google
- Applications : Salesforce

LICENCES ET BREVETS

La spécification FIDO est propriété du consortium FIDO Alliance™. Les documents relatifs aux différents protocoles définis sont librement accessibles sur le site de l'Alliance et ne font l'objet d'aucune redevance. L'implémentation d'un protocole n'est soumise à aucune exigence commerciale, seule la certification d'un produit est payante.

ACTEURS PROMOUVANT CETTE TECHNOLOGIE

La liste des membres de l'Alliance est disponible sur leur site internet : https://fidoalliance.org/members/.

L'Alliance a également de nombreux accords d'échange avec d'autres associations influentes : Bluetooth, ETA, Eurosmart, EMVCo, ou encore le W3C (voir liste https://fidoalliance.org/members/liaison/).

Cryptographie post quantique

DESCRIPTION DE LA TECHNOLOGIE

Les progrès de la seconde révolution des technologies quantiques laissent entrevoir l'avènement probable de l'ordinateur quantique dans le futur. Même s'il n'est pas encore certain qu'il puisse jamais voir le jour, cette possibilité doit être sérieusement prise en compte dès aujourd'hui au vu des graves conséquences qu'un tel évènement pourrait avoir.

La cryptographie post quantique ou « Quantum Safe Cryptography » (QSC) désigne la cryptographie résistante à l'ordinateur quantique, appelée à remplacer l'actuelle cryptographie asymétrique comme le RSA ou la cryptographie sur courbe elliptique.

Quelles conséquences de l'avènement de l'ordinateur quantique ?

En effet, un ordinateur quantique rendrait possible la mise en œuvre de méthodes de cryptanalyse nouvelles qu'il n'est par nature pas possible de réaliser sur les ordinateurs classiques. Ces méthodes pourraient alors casser toute la cryptographie asymétrique classique actuellement utilisée (telle que le RSA ou la cryptographie sur courbe elliptique).

En particulier, l'ordinateur quantique permettrait d'appliquer l'algorithme de Shor, permettant de résoudre les problèmes mathématiques considérés comme difficiles que sont (1) la factorisation de grands nombres, ou (2) le logarithme discret en beaucoup moins d'opérations (et donc de manière beaucoup plus rapide et efficace) que ce qu'il est possible de faire avec un ordinateur classique. Cette faculté tient à la nature intrinsèque de l'ordinateur quantique qui repose sur des propriétés quantiques sous-jacentes, et non à une capacité de calcul accrue. Or ces deux problèmes mathématiques sont à la base de toute la cryptographie asymétrique utilisée aujourd'hui : factorisation de grands nombres pour le RSA, logarithme discret pour le DSA, le DH et la cryptographie sur courbe elliptique.

Alors que cela peut sembler assez technique, les conséquences seraient très visibles. Toute la sécurité numérique repose sur l'utilisation de la cryptographie classique pour assurer les services de sécurité suivants :

- **Authentification** en ligne des ordinateurs, des serveurs et des personnes pour s'assurer qu'il ne s'agit pas d'une entité/personne non autorisée ;
- **Chiffrement** des données afin d'assurer leur confidentialité ;
- **Signature numérique** pour matérialiser le consentement irrévocable et opposable d'une personne à un acte ou un contrat ;

- **Sceau numérique** garantissant l'intégrité (non modification) et l'authenticité (origine) d'une donnée ou d'un programme ;

Casser la cryptographie asymétrique actuellement utilisée reviendrait à réduire à néant ces propriétés de sécurité et partant toute la confiance numérique. Les conséquences seraient désastreuses.

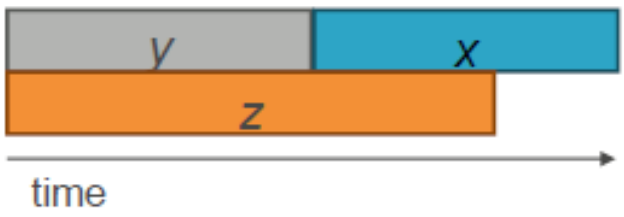
Le sujet est devenu d'actualité en 2015, lorsque la direction de la sécurité de l'information (Information Security Directorate) de la NSA a indiqué souhaiter migrer vers une cryptographie résistante à l'ordinateur quantique à un horizon pas trop éloigné (« *not too distant future* »). Cette prise de position officielle a attiré l'attention de tous sur la nécessité de préparer dès que possible cette transition.

Quels risques ?

La mise au point d'un ordinateur quantique apte à casser la cryptographie asymétrique actuelle prendra certainement encore beaucoup de temps, si tant est qu'il puisse jamais voir le jour, même si de nombreux pronostiqueurs se risquent à formuler des prédictions alarmistes (une chance sur sept de casser le RSA 2048 bits d'ici 2026, une chance sur deux d'ici 2030 (2015), 20 qubits dans 20 ans (1996), …). Toutefois, même si son apparition prendra beaucoup de temps, il faut s'en préoccuper dès maintenant et préparer la migration vers la cryptographie post quantique dès aujourd'hui.

Une des principales menaces à considérer est celle d'un attaquant qui vole des données chiffrées (par exemple des données stockées sur un serveur qui sont volées via une cyber-attaque), les conserve, puis les déchiffre dès qu'un ordinateur quantique apte à casser la cryptographie asymétrique classique est disponible. En effet, beaucoup de données conservent une valeur même plusieurs années après leurs vols (numéros de carte bancaire, coordonnées bancaires, mots de passe, données stockées en nuage, données d'entreprise...). Sur une échelle de temps, les durées suivantes peuvent être représentées :

- X la durée requise de protection des données pendant laquelle leur confidentialité doit être assurée ;
- Y la durée nécessaire pour organiser la migration des systèmes vers une cryptographie post quantique ;
- Z le temps nécessaire à la mise au point d'un ordinateur quantique apte à casser la cryptographie asymétrique classique ;



La confidentialité des données est assurée tant que **X + Y < Z** : la durée requise de protection des dernières données chiffrées avec la cryptographie asymétrique classique expire avant la mise au point d'un ordinateur quantique.

La confidentialité des données est compromise dès lors que **X + Y > Z** : la durée requise de protection des dernières données chiffrées avec la cryptographie asymétrique classique dépasse la date de mise au point d'un ordinateur quantique. Par conséquent, les données chiffrées à la fin de la période de migration seront compromises avant l'expiration de leur durée requise de protection.

Si **Y > Z**, la durée de migration de systèmes dépasse le temps nécessaire à la mise au point de l'ordinateur quantique. Cela signifie un possible effondrement généralisé des infrastructures.

La cryptographie asymétrique actuelle (telle que le RSA ou la cryptographie sur courbe elliptique), qui est largement utilisée, a mis plus de 30 ans à se déployer, entre la conception des algorithmes (brevet du RSA déposé en 1977) et utilisation à grande échelle avec le développement d'internet (début des années 2000). Par conséquent, il est raisonnable de considérer qu'il en sera de même avec la cryptographie post quantique (Y = 30 ans).

Pour ce qui est de la durée requise de protection des données, une période de 5 à 10 ans parait raisonnable (X = 5-10 ans).

Par conséquent, afin de garantir la protection des données et éviter leurs compromissions, il faut que **X + Y < Z**, soit **Z > 35-40 ans**.

Au vu des progrès technologiques énormes que nous avons vécu au cours des dernières décennies, il n'est pas à exclure que d'ici 35 ans (1) l'ordinateur quantique ait été inventé, et (2) qu'il puisse casser la cryptographie asymétrique classique.

Quelles solutions ?

Une nouvelle génération de cryptographie asymétrique insensible à l'algorithme de Shor est donc nécessaire. Comme ce dernier permet de résoudre les problèmes mathématiques de la factorisation de grands nombres et du logarithme discret, qui sont la base de la cryptographie asymétrique classique (telle que le RSA ou la cryptographie sur courbe elliptique), cela implique de bâtir une nouvelle génération de cryptographie asymétrique basée sur d'autres problèmes mathématiques.

Plusieurs familles d'algorithmes post quantiques, basées sur d'autres problèmes mathématiques non affectés par l'algorithme de Shor ont été identifiées pour succéder à la cryptographie asymétrique classique :

- Cryptographie sur réseaux euclidiens (« Lattice-based cryptography ») ;
- Cryptographie sur les codes (« Code-based cryptography ») ;
- Cryptographie multivariée (« Multivariate-based cryptography ») ;
- Cryptographie à base de fonction de hachage (« Hash-based cryptography ») ;
- Cryptographie à base d'isogénie de courbes elliptiques supersingulières (« Isogeny-based cryptography ») ;

Quid de la cryptographie symétrique ?

La cryptographie symétrique, de type DES ou AES, est, elle aussi, affectée par l'ordinateur quantique, mais dans une moindre mesure.

Dans l'état actuel des connaissances, seul l'algorithme de Grover lui est applicable. Toutefois, alors que l'algorithme de Shor promet de réduire à néant la sécurité de la cryptographie asymétrique classique car il s'attaque aux fondements mathématiques sous-jacents, la situation est différente pour la cryptographie symétrique. L'algorithme de Grover n'attaque pas les fondements mathématiques sous-jacents de la cryptographie symétrique, mais permet d'accélérer la seule attaque possible connue qui est la recherche exhaustive de la valeur de la clef.

Une clef de n bits peut prendre 2^n valeurs possibles, nécessitant autant de tentatives pour retrouver sa valeur en procédant à une recherche exhaustive avec un ordinateur classique. Grâce à l'algorithme de Grover exécuté sur un ordinateur quantique, il est possible d'optimiser cette recherche exhaustive et de retrouver la valeur de la clef en $2^{n/2}$ tentatives.

Ce nombre de tentatives nécessaires pour retrouver la valeur de la clef symétrique permet de mesurer le niveau de résistance de la cryptographie symétrique. Ainsi, là où un algorithme symétrique a un niveau de sécurité de n bits (par exemple 128 bits pour l'AES-128) en l'absence d'ordinateur quantique, il sera de n/2 bits dans l'hypothèse où l'algorithme de Grover deviendrait applicable (64 bits pour l'AES-128).

Ainsi la cryptographie symétrique reste actuellement considérée comme résistante à l'ordinateur quantique. Il suffit simplement d'ajuster la taille de clef symétrique afin de conserver le même niveau de résistance, en doublant sa taille.

Toutefois cette analyse reste encore à confirmer par des travaux de recherches, en particulier pour s'assurer qu'il n'existe pas d'autres attaques quantiques, découlant des nouvelles possibilités de cryptanalyse qui seront permises par les capacités de l'ordinateur quantique, applicables à la cryptographie symétrique.

MATURITE

Plusieurs familles d'algorithmes post quantiques ont été identifiées à ce jour pour succéder aux algorithmes asymétriques actuellement utilisés (tels que le RSA et la cryptographie sur courbe elliptique).

Hormis la cryptographie à base de fonction de hachage qui fait l'objet d'un consensus académique quant à sa sécurité face à l'ordinateur quantique et aux attaques classiques, les autres familles d'algorithmes doivent encore faire l'objet de travaux de recherche pour (1) les améliorer (temps d'exécution, taille de clefs et de signature…) et (2) évaluer leurs sécurités.

La cryptographie à base de fonction de hachage présente un certain nombre de limitations majeures qui font qu'elle ne peut à elle seule répondre au défi de l'ordinateur quantique et remplacer les algorithmes asymétriques actuellement utilisés. Il est donc nécessaire de disposer d'autres familles d'algorithmes post quantiques.

À ce jour, aucun des algorithmes post quantiques (hormis certains basés sur les fonctions de hachage) ne sont reconnus comme sûrs par la communauté scientifique et les agences de sécurité nationales. Ceux-ci étant appelés à remplacer les algorithmes actuels (tels que le RSA et la cryptographie sur courbe elliptique) et donc à être utilisés pour des usages très sensibles, il est nécessaire de s'assurer qu'ils sont exempts de tout défaut de conception ou de failles pouvant constituer des faiblesses exploitables par des personnes malveillantes. Cette assurance s'acquiert au travers d'un processus transparent de revue par les pairs chercheurs en cryptographie et nécessite donc (1) des travaux de recherche fondamentale pour étudier les algorithmes, et (2) un dialogue au sein de la communauté.

En particulier, la recherche doit étudier de manière approfondie les attaques quantiques applicables à chacune de ces familles d'algorithmes, découlant des nouvelles possibilités de cryptanalyse qui seront permises par les capacités de l'ordinateur quantique. Ainsi par exemple, l'algorithme RSA et de la cryptographie à courbe elliptique, sont sensibles à une attaque quantique utilisant l'algorithme de Shor. Une tâche essentielle de la recherche fondamentale est de s'assurer que les algorithmes post quantiques ne sont sensibles à aucune attaque quantique.

Cryptographie sur réseaux euclidiens (« Lattice-based cryptography »)

Cette famille d'algorithme est étudiée depuis plus de vingt ans et il s'agit d'un domaine de recherche très actif avec des groupes de travail spécifiques et de nombreuses publications.

Par ailleurs la recherche fondamentale est soutenue par une compétition lancée par l'université technologique de Darmstadt en 2015, visant à mettre en défaut la sécurité des problèmes sur réseaux euclidiens.

La résistance de cette famille aux attaques quantiques a commencé à être étudiée au cours des dernières années.

Cryptographie sur les codes (« Code-based cryptography »)

Cette famille d'algorithme est étudiée depuis plus de quarante ans et il s'agit d'un domaine de recherche très actif avec des groupes de travail spécifiques et un flux faible mais constant de publications.

La résistance de cette famille aux attaques quantiques a aussi fait l'objet d'étude au cours des dernières années.

Cryptographie multivariée (« Multivariate-based cryptography »)

Cette famille d'algorithme est étudiée depuis plusieurs dizaines d'années et fait actuellement l'objet de groupes de travail spécialisés, de travaux de recherche et de nombreuses publications.

La recherche fondamentale est soutenue par une compétition lancée en 2015 visant à casser cette famille d'algorithmes. À ce jour, les attaques classiques (non quantiques) sur cette famille d'algorithme font encore l'objet de travaux de recherche actifs.

La confiance dans les algorithmes de mise en accord de clefs de cette famille a été considérablement amoindrie, car des travaux de recherche ont démontré la faiblesse de nombreux schémas de ce type proposés au cours des dernières années. Les algorithmes de signature bénéficient d'une confiance un peu supérieure, bien que des travaux de recherche aient démontré la faiblesse de certains d'entre eux.

Par ailleurs, la résistance de cette famille d'algorithme aux attaques quantiques est encore un sujet vierge qui doit faire l'objet de travaux de recherche.

Cryptographie à base de fonction de hachage (« *Hash-based cryptography* »)

Cette famille d'algorithme a été introduite par les travaux de Merkle à la fin des années 1970 sur des schémas de signature à base de fonction de hachage. Le schéma de signature de Merkle est à présent bien compris et considéré comme très sûr. Toutefois, il est peu commode à mettre en œuvre car il est dit « *stateful* », c'est-à-dire avec un état interne. En effet, la nature de l'algorithme impose d'utiliser des bi-clefs de signature à usage unique devant être renouvelées après toute signature, si bien qu'un état interne de l'algorithme est nécessaire, correspondant

à la bi-clef de signature à utiliser pour une opération donnée dans une liste prédéfinie. Néanmoins, cette spécificité peut être masquée de sorte à ne présenter globalement qu'une clef publique aux tiers désireux de vérifier la signature cryptographique.

Les travaux de recherche actuels se concentrent sur une amélioration de ce schéma de signature de sorte à le rendre « *stateless* », c'est-à-dire avec une bi-clef de signature à usage multiple.

Les schémas de signature dit « stateful » sont très matures si bien qu'ils ont pu faire l'objet d'initiatives de normalisation précoces dès les années 2010 (cf. travaux de l'IETF). De plus, le NIST a officiellement indiqué en octobre 2020 que certains schémas de signature à base de fonction de hachage (plus précisément LMS et XMSS) sont résistants à l'ordinateur quantique. Cette prise de position pose le premier jalon d'une migration des usages vers une cryptographie post quantique, et ce dès que possible, avant la conclusion de la compétition organisée par le NIST, permettant aux usages les plus menacés d'engager rapidement une migration vers une cryptographie post quantique. Il n'en reste pas moins qu'il ne s'agit ici que d'une première marche, imparfaite et inachevée, car cette cryptographie n'offre qu'une primitive de signature.

L'efficacité des attaques quantiques sur cette famille d'algorithme a été largement étudiée et est à présent bien connue.

Par ailleurs, il faut noter que cette famille d'algorithme permet de réaliser uniquement des signatures, et ne permet pas de réaliser des mises en accord de clefs ou du chiffrement.

Cryptographie à base d'isogénie de courbes elliptiques supersingulières (« Isogeny-based cryptography »)

Cette famille d'algorithme est la plus récente et est apparue il y a environ dix ans. Il s'agit d'un domaine de recherche relativement nouveau. Des travaux de recherches sont encore nécessaires afin de bâtir un consensus académique sur les propriétés de sécurité de cette famille d'algorithmes.

La recherche sur cette famille d'algorithmes n'est pas actuellement soutenue par une compétition visant à la mettre en défaut.

COMPETITION LANCEE PAR LE NIST

C'est dans ce contexte que le NIST a lancé en 2016 une « compétition internationale » avec un double objectif : (1) définir et identifier des algorithmes post quantiques sûrs, et (2) en standardiser certains[41]. En organisant cette

[41] https://csrc.nist.gov/projects/post-quantum-cryptography

compétition, le NIST souhaite fédérer les efforts de recherche de la communauté scientifique. En effet, il juge que la mise au point d'algorithmes sûrs requiert encore beaucoup d'efforts de recherche, que les seules structures de normalisation (e.g. ISO) ne sont pas à même de stimuler et d'organiser.

Cette compétition va permettre (1) la mise à disposition de tous d'algorithmes reconnus comme sûrs, et (2) la publication par le NIST de standards techniques portant sur un ou quelques algorithmes choisis parmi ces derniers par le NIST.

À l'issue de cette compétition, les applications faisant usage de cryptographie asymétrique, pourront organiser leur migration vers des algorithmes post quantiques résistants à l'ordinateur quantique.

Le NIST prévoit la fin de cette compétition en 2022/2023 avec la publication d'un standard technique.

Il faut noter que cette compétition n'interdit pas aux soumissionnaires de breveter leurs propositions, et ne garantit en rien que les algorithmes lauréats et standardisés soient exempts de brevets.

Périmètre de la compétition

La compétition porte uniquement sur les algorithmes asymétriques (dit à clef publique), et non les algorithmes symétriques ou les fonctions de hachage.

La compétition s'intéresse en particulier aux trois primitives asymétriques de base suivantes :

- **Signature**. Ce type d'algorithme permet de créer une signature numérique d'un message à partir d'une clef privée, la signature numérique pouvant quant à elle être vérifiée à l'aide de la clef publique correspondante.
- **Mise en accord de clefs**. Ce type d'algorithme permet à deux parties ne se connaissant pas à priori, et possédant chacune une paire de clefs asymétriques (privée et publique), de générer un secret commun, uniquement connu d'elles seules, en échangeant uniquement leurs clefs publiques. Ce type d'algorithme permet par exemple à deux parties d'initier une communication sécurisée.
- **Chiffrement**. Ce type d'algorithme permet à quiconque possédant la clef publique d'un destinataire de chiffrer un message à son intention, que lui seul pourra consulter à l'aide de sa clef privée. Ces algorithmes sont en général distincts des algorithmes de signature (e.g. EC-DSA).

Le NIST a par ailleurs défini cinq niveaux de résistance pour évaluer les algorithmes proposés, décrit ci-dessous :

Niveau	Description du niveau de résistance	Modèle d'attaque
1	Au moins aussi dur à casser que l'AES-128	Recherche exhaustive de clef
2	Au moins aussi dur à casser que le SHA-256	Recherche de collision
3	Au moins aussi dur à casser que l'AES-192	Recherche exhaustive de clef
4	Au moins aussi dur à casser que le SHA-384	Recherche de collision
5	Au moins aussi dur à casser que l'AES-256	Recherche exhaustive de clef

Le NIST a demandé aux soumissionnaires de se focaliser sur les trois premiers niveaux de résistance (1,2 et 3). Ces trois niveaux correspondent à la majorité des usages civils (usages de masse et commerciaux), pour lesquels le besoin de standardisation d'algorithmes est le plus prégnant.

Les deux derniers niveaux de résistance (4 et 5) correspondent plutôt à des usages exigeants de hauts niveaux de sécurité (e.g. gouvernementaux ou militaires). Ces usages sont moins susceptibles de faire appels à des algorithmes standardisés, mais plutôt à des algorithmes secrets ou visés par les autorités nationales de sécurité de l'information du pays.

Critères de choix

Les deux principaux critères pris en compte pour la sélection des algorithmes proposés sont :

- **Sécurité et résistance** contre les attaques classiques connues, mais aussi les attaques quantiques. Ces dernières recouvrent bien sûr l'algorithme de Shor, mais aussi toute méthode de cryptanalyse pouvant s'exécuter sur un ordinateur quantique. En effet, l'avènement de l'ordinateur quantique promet des avancées dans la théorie des nombres sur laquelle repose toute la cryptographie ;
- **Performance** d'exécution sur diverses plateformes (architecture matérielle, logicielle…) ;

Par ailleurs d'autres critères sont aussi pris en compte :

- **Substituable de manière transparente**. Il s'agit de l'aptitude d'un algorithme à pouvoir remplacer un autre dans une implémentation typique (principalement le SSL/TLS ou le protocole IKE) de la manière la plus transparente pour les couches supérieures en faisant l'utilisation. Cela implique en particulier que les signatures et les clefs publiques aient sensiblement la même taille, et que le temps d'exécution soit proche.
- **Résistance aux attaques par canaux auxiliaires.** Ces attaques consistent à mesurer l'information fuitant au cours de l'exécution de l'algorithme au travers des canaux auxiliaires (consommation de courant, rayonnement électromagnétique, temps d'exécution, signaux caractéristiques…) puis à l'analyser pour en extraire des informations sur la clef privée manipulée. Ce type d'attaque est inhérent à toute implémentation matérielle ou logicielle d'un algorithme, et doit être pris en compte dès lors qu'un attaquant est capable de mesurer certains de ces canaux auxiliaires (consommation, temps d'exécution…).
- **Simplicité et flexibilité** ;
- **« Perfect forward secrecy »**. Cette propriété s'applique aux algorithmes de mise en accord de clef utilisés pour générer des clefs de session (e.g. clef de chiffrement). Cette propriété garantit que si une clef privée utilisée pour générer les clefs de session est corrompue, les clefs de session resteront quant à elles non compromises. Concrètement, cela assure que tous les messages passés, chiffrés avec les clefs de session, restent protégés si dans le futur la clef privée utilisée pour générer les clefs de session est corrompue.

Résultats du troisième tour

De nombreux algorithmes candidats ont été proposés au NIST par des équipes internationales réunissant tout à la fois le milieu académique et industriel.

À l'issue du troisième tour de sélection, à la mi 2020, le jury scientifique du NIST a retenu deux catégories d'algorithmes :

- **Des algorithmes finalistes**, qui semblent prometteurs, et qui feront l'objet d'une publication par le NIST vers 2022-2023 ;
- **Des algorithmes alternatifs,** qui semblent eux aussi prometteurs, mais nécessitent encore un travail de revue approfondie par la communauté, et feront peut-être l'objet d'une publication par le NIST dans un second temps ;

Les algorithmes retenus à l'issue du troisième tour sont les suivants :

Familles de problèmes mathématiques	**Type d'algorithme**		
	Signature	Mécanisme de chiffrement de clefs	Total
Cryptographie sur réseaux euclidiens (« Lattice-based »)	**-Crystals-Dilithium** **-Falcon**	**-Crystals-Kyber** **-NTRU** **-Saber** Alternatifs : -FRODOKEM -NTRUPrime	5 (finalistes)
Cryptographie sur les codes (« Code-based »)	-	**-Classic McEliece** Alternatifs : -HQC -BIKE	1 (finaliste)
Cryptographie multivariée (« Multivariate-based cryptography »)	**-Rainbow** Alternatif : -GeMSS	-	1 (finaliste)
Cryptographie à base de fonction de hachage (« Stateless Hash-based/Symmetric based »)	Alternatifs : -PicNic -SPHINCS+	-	0 (finaliste)
Isogenie de courbe elliptique supersingulière	-	Alternatif : -SIKE	0 (finaliste)

Il apparait clairement que la cryptographie sur réseaux euclidiens (« Lattice-based ») est la plus prometteuse. Elle représente 5 des 7 algorithmes finalistes, et est la seule pour laquelle des primitives de signature et de chiffrement de clefs sont disponibles.

Prochaines étapes

Les algorithmes retenus à l'issue du troisième tour (finalistes et alternatifs) feront l'objet de revue, d'analyse et de commentaires par la communauté scientifique, menant à des modifications éventuelles de ces derniers. La publication du projet de rapport technique standardisant les algorithmes finalistes est prévu pour 2022-2023. La publication de la version finale du rapport technique aura lieu quant à elle à une date ultérieure.

Les algorithmes alternatifs – ou du moins certains d'entre eux – feront l'objet de la publication d'un autre rapport technique. Celui-ci sera publié dans un second temps, après la publication du rapport technique décrivant les algorithmes finalistes. La date de publication n'est pas connue à ce jour.

DEPLOIEMENT ET UTILISATION SUR LE TERRAIN

Il ne semble pas y avoir de déploiement et d'utilisation sur le terrain d'algorithmes post quantiques. Néanmoins, quelques expérimentations ont eu lieu.

Expérimentation faite par Google

En 2016, Google a lancé une expérimentation au cours de laquelle un algorithme post quantique combiné à un algorithme standard fut utilisé pour sécuriser la communication entre une fraction de postes clients équipés du navigateur Chrome et les serveurs de Google. L'algorithme utilisé était « New Hope » (cryptographie sur réseaux euclidiens « lattice-based ») qui permet une mise en accord de clef.

Au cours de cette expérimentation, une implémentation de « New-Hope » a été réalisée sur le navigateur Chrome et aussi sur des HSMs (pour les serveurs).

Expérimentation faite par Microsoft

Microsoft a rendu public le projet « PQCrypto-VPN » qui propose un logiciel libre enrichissant « OpenVPN » avec des algorithmes post quantiques (« OpenVPN » est une solution logicielle libre permettant de créer des réseaux privés virtuels entre ordinateurs).

Ce projet étend « OpenVPN » en y ajoutant les trois algorithmes post quantiques suivants proposés à la compétition du NIST et dont Microsoft est co-auteur :

- FrodoKEM (mise en accord de clef) ;

- SIKE (chiffrement, mise en accord de clef) ;
- PicNic (signature) ;

Le projet « PQCrypto-VPN » est disponible sur github et peut être utilisé par tous (https://github.com/Microsoft/PQCrypto-VPN)

CONTRAINTES

Les contraintes principales des algorithmes post quantiques portent essentiellement sur (1) la taille des clefs, (2) la taille de signature, (3) le temps d'exécution, (4) le temps de génération des bi-clefs, et (5) l'espace mémoire nécessaire à l'exécution de l'algorithme. Ces paramètres varient grandement en fonction de l'algorithme considéré, même au sein de la même famille.

Par ailleurs, certaines familles d'algorithmes présentent des probabilités d'erreur non nulles au cours des opérations de déchiffrement. Cela signifie que de manière aléatoire, les algorithmes peuvent ne pas parvenir à déchiffrer un message.

La cryptographie à base de fonction de hachage présente pour sa part des contraintes spécifiques. Elle n'offre que des primitives cryptographiques de signature, et pas de primitives cryptographiques de déchiffrement et de mise en accord de clefs.

NORMALISATION

ISO (Organisation internationale de normalisation)

L'ISO/IEC JTC1/SC27/WG2 (« Cryptography and security mechanisms ») a lancé dès octobre 2015, un appel à contribution sur le sujet auprès de la communauté, lequel a duré 2 ans. À l'issue de cette période, un consensus s'est alors dégagé sur l'urgence pour le WG2 de préparer la normalisation de cette nouvelle génération d'algorithme. Le WG2 a alors lancé la préparation du document ISO/IEC SD8 (ISO Standing Document 8).

Ce document n'est pas un standard, mais plutôt un document de référence (guide). Il vise non pas à normaliser des algorithmes post quantiques, mais à préparer la communauté à contribuer en mettant à sa disposition un document (1) présentant chacune des familles d'algorithme post quantique, et pour chacune (2) précisant comment évaluer correctement les algorithmes (sécurité, performance…). Ce document est un guide pour préparer la prochaine étape de normalisation qui portera sur les algorithmes post quantiques eux-mêmes.

À titre d'illustration, des algorithmes post quantiques pourront être inclus dans ce document, après revue et analyse par le groupe d'experts. Toutefois, ce document n'a absolument pas vocation à servir de support de normalisation à des

algorithmes post quantiques, car (1) ce document ne sera pas un standard, et (2) les algorithmes seront inclus uniquement comme exemples.

Ce document se décompose en 8 parties

- Partie 1 : General ;
- Partie 2 : Signature basée sur des fonctions de hachage « Hash-based signature » (publication prévue en automne 2018) ;
- Partie 3 : Cryptographie sur réseaux euclidiens « Lattice-based » (publication prévue au printemps 2019) ;
- Partie 4 : Cryptographie sur codes « Coding-based » (publication prévue en automne 2019) ;
- Partie 5 : Cryptographie multivariée « Multivariate » (publication prévue au printemps 2020) ;
- Partie 6 : Cryptographie à base d'isogenie de courbe elliptique supersingulière « Elliptic curve isogeny » ;

European Telecommunication Standardisation Institute (ETSI)

Le sujet est traité par le groupe de travail WG QSC (Working Group on Quantum Safe Cryptography) au sein du TC Cyber (Technical Committee on cybersecurity). Ce groupe de travail résulte de la transformation en 2017 de l'ISG QSC (Industry Specification Group on Quantum Safe Cryptography) qui a été créé en 2015.

Ce groupe de travail n'a pas pour but de développer ou définir de nouveaux algorithmes post quantiques, mais de se focaliser sur leurs mises en œuvre pratiques. Ses travaux ont vocation à alimenter les autres groupes ou projets de l'ETSI (e.g. 3GPP), ou d'autres organismes de normalisation (IETF, ITU…).

Les rapports techniques suivants ont été publiés par ce groupe :

- ETSI GR QSC001 Analysis of Quantum-Safe Primitives;
- ETSI GR QSC003 Quantum-Safe Case Studies & Use Cases;
- ETSI GR QSC004 Quantum-Safe Threat Analysis;
- ETSI GR QSC006 Limits of Quantum Computing on Symmetric Key Cryptography;
- ETSI TR 103 570 Quantum-Safe Key Exchanges, Implementation Analysis ;
- ETSI TR 103 617 Quantum-Safe Virtual Private Network (VPN);

Par ailleurs, les rapports techniques suivants sont aussi en préparation au sein de ce groupe :

- QSC-008: Quantum-Safe Cryptographic Signature assessment ;
- QSC-12: Quantum-Safe Identity-Based Encryption (IBE);

- QSC-13: Migration Techniques to Quantum-Safe Systems;

Institute of Electrical and Electronics Engineers (IEEE)

L'IEEE (Institute of Electrical and Electronics Engineers) a publié en 2009 la norme **P1363.3** qui décrit un schéma (1) de chiffrement asymétrique, (2) signature et (3) mise en accord de clef basé sur des réseaux euclidiens (« lattice-based »).

Internet Research Task Force (IETF)

L'IETF (Internet Research Task Force) a normalisé les deux schémas de signature à base de fonction de hachage avec état interne (« stateful hash-based ») reconnus résistant à l'ordinateur quantique par le NIST :

- Le schéma e**X**tended **M**erkle **S**ignature **S**cheme (XMSS) décrit dans la RFC 8391 en 2018 ;
- Le schéma **L**eighton-**M**icali **S**ignature (LMS) décrit dans la RFC 8559 en 2019 ;

Ainsi que d'autres documents permettant le déploiement et l'utilisation du schéma de signature Leighton-Micali (algorithme de signature à base de fonction de hachage) dans les applications internet :

- **RFC 8708 - Use of the HSS/LMS Hash-Based Signature Algorithm in the Cryptographic Message Syntax (CMS).** Ce document vise à permettre l'utilisation du schéma de signature LMS dans les structures de données de type Cryptographic Message Syntax (CMS) ;
- **RFC 8778 - Use of the HSS/LMS Hash-Based Signature Algorithm with CBOR Object Signing and Encryption (COSE).** Ce document vise à décrire l'utilisation du schéma de signature LMS pour les structures de données de type CBOR Object Signing and Encryption (COSE). Ces structures de données sont utilisées pour transmettre des données formatées en CBOR, protégées en confidentialité (chiffrées), intégrité et authenticité (signées). Elles servent en particulier à sécuriser la distribution des mises à jour logicielles.

Par ailleurs, l'IETF prépare actuellement plusieurs documents visant à mettre à jour les protocoles et mécanismes de sécurité actuellement utilisés par internet afin d'y introduire la possibilité de les utiliser avec des algorithmes post quantiques :

- **Hybrid ECDHE-SIDH Key Exchange for TLS.** Ce document vise à spécifier une variante du protocole TLS combinant la cryptographie sur courbe elliptique, et des isogénies de courbes elliptiques supersingulières ;
- **Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS).** Ce document vise à spécifier un échange de clef hybride pour le protocole TLS v1.2 combinant (1) la

cryptographie sur courbe elliptique et (2) un mécanisme de chiffrement de clef résistant à l'ordinateur quantique, comme BIKE ou SIKE (utilisant des isogénies de courbes elliptiques supersingulières) ;

- **Design issues for hybrid key exchange in TLS 1.3.** Ce document discute des considérations de conception pour l'utilisation d'échange de clef hybrides dans le protocole TLS v1.3 ;
- **Multiple Public-Key Algorithm X.509 Certificates.** Ce document vise à spécifier un format de certificat X509, liste de révocation (CRL) et fichier P10 contenant deux matériaux cryptographiques. Il a pour but de permettre la migration d'une PKI basée sur une cryptographie asymétrique classique vers une PKI à base de cryptographie résistante à l'ordinateur quantique ;
- **Framework to Integrate Post-quantum Key Exchanges into Internet Key Exchange Protocol Version 2 (IKEv2).** Ce document vise à étendre le protocole IKEv2 pour permettre l'utilisation d'algorithmes post quantiques de mise en accord de clef ;

National Institute of Standards and Technology (NIST)

Le National Institute of Standards and Technology (NIST) a publié en octobre 2020 le document SP 800-208 « Recommendation for Stateful Hash-Based Signature Schemes". Ce document (1) recommande l'utilisation des algorithmes LMS (Leigthon-Micali Signature) et XMSS (Extended Merkle Signature Scheme) par les services fédéraux américains, et (2) reconnait leurs résistances à l'ordinateur quantique – sous certaines hypothèses.

CAS D'USAGES IDENTIFIES

Toutes les applications reposant sur des algorithmes asymétriques sont appelées à terme à migrer vers des algorithmes post quantiques. Ainsi, les infrastructures à clefs publiques (PKI), les blockchains, les services de signature électronique, les protocoles de sécurisation web TLS/SSL… sont appelés à migrer vers des algorithmes post quantiques.

LICENCES ET BREVETS

Certaines familles d'algorithmes post quantiques reposent sur des problèmes étudiés depuis de nombreuses années. Aussi il est fort probable que des brevets couvrent certains d'entre eux ou certaines méthodes d'optimisation ou de sécurisation contre les attaques par canaux auxiliaires.

Par ailleurs, le processus mis en place par le NIST pour sélectionner des algorithmes post quantiques sûrs n'interdit en rien de proposer des algorithmes brevetés, ou dont des modes de réalisation optimisés et/ou sécurisés sont brevetés. Ainsi, au moins 10 propositions faites au NIST ont été déclarées comme étant brevetées.

ACTEURS PROMOUVANT CETTE TECHNOLOGIE

Une analyse rapide des réponses faites à la compétition du NIST fait apparaitre quelques tendances fortes.

Tout d'abord, la plupart des réponses associent à la fois des entreprises et des centres de recherches. Il y a assez peu de réponses issues uniquement du monde académique. Cela démontre l'intérêt des entreprises pour le sujet.

Entreprises

Les entreprises participant à cette compétition sont essentiellement issues soit du domaine de l'informatique en nuage, soit du domaine du semi-conducteur.

Dans le premier cas, il s'agit bien entendu de permettre un stockage sécurisé de données à très long terme sur des serveurs. Ceci est d'autant plus capital qu'il n'est malheureusement pas possible de garantir une protection totale des données en nuage contre le vol. Il faut donc disposer d'un moyen de chiffrement résistant à long terme assurant que même des données chiffrées volées restent inexploitable pour l'attaquant.

Dans le second cas, il s'agit de permettre une exécution efficace des algorithmes post quantiques sur des semi-conducteurs.

Centres de recherche

Les centres de recherches impliquées proviennent en majorité (1) d'Amérique du nord (États-Unis, Canada), (2) de quelques pays d'Europe (principalement Allemagne, France, Danemark, Pays-Bas et Suisse), (3) de quelques pays d'Asie (Singapour, Japon, Corée du Sud, Chine), et (4) d'Australie.

Par ailleurs, face à ce défi que constitue l'ordinateur quantique et la nécessité de développer une nouvelle génération d'algorithmes résistants, certains pays ont développé des stratégies nationales.

États Unis

Le pays a été le premier à alerter sur les risques de l'ordinateur quantique pour la cryptographie classique, et sur la nécessité de préparer la migration vers une cryptographie post quantique. En effet, en 2015, la direction de la sécurité de l'information (Information Security Directorate) de la NSA a indiqué souhaiter migrer vers une cryptographie résistante à l'ordinateur quantique à un horizon pas trop éloigné (« *not too distant future* »).

Par ailleurs, le pays, au travers du NIST, est l'initiateur de la compétition visant à accélérer la définition et la normalisation des algorithmes post quantiques. Le NIST

a aussi proposé plusieurs (co-) éditeurs pour la rédaction du Standing Document 8 (SD8) préparé par le SC27/WG2.

Par ailleurs de nombreuses entreprises privées investissent dans le domaine.

France

La France a lancé une initiative pour développer et structurer les efforts de l'industrie et des centres de recherche nationaux dans le domaine de la cryptographie post quantique. Le projet industriel RISQ - **R**egroupement de l'**I**ndustrie française pour la **S**écurité Post-**Q**uantique (risq.fr), réunissant un consortium d'industriels (7) et de centres de recherche (7) a ainsi reçu un financement de 7,45 millions d'euros pour une période de 3 ans (avril 2017-avril 2020) au titre du programme d'investissement d'avenir (PIA). L'objectif de ce projet industriel financé est de faire de la France un acteur majeur de la transition post quantique.

Les livrables attendus de ce projet sont de plusieurs ordres :

- Conception d'algorithmes post quantiques ;
- Conception de briques cryptographiques matérielles et logicielles ;
- Mise à disposition d'une gamme complète de produits de signature et chiffrement ;
- Adaptation du protocole internet TLS ;
- Mise à disposition de documentation permettant d'accompagner l'industrie dans la migration vers les algorithmes post quantiques ;
- Participation à la normalisation internationale ;

Le projet industriel RISQ a permis de bien positionner la recherche française au niveau mondial. Ainsi, les participants au projet industriel RISQ, seuls ou en collaboration avec des partenaires étrangers, sont à l'origine de 9 propositions soumises à la compétition du NIST sur 69, soit 13%, mais surtout de 3 algorithmes finalistes (sur 7) et 2 algorithmes alternatifs (sur 8) à l'issue du troisième tour de la compétition organisée par le NIST.

Il s'agit des algorithmes suivants :

- CFKPM (mise en accord de clefs) ;
- CRYSTALS-Dilithium (signature) – retenu comme finaliste à l'issue du troisième tour ;
- CRYSTALS-Kyber (chiffrement) – retenu comme finaliste à l'issue du troisième tour ;
- DualModeMS (signature) ;
- Falcon (signature) – retenu comme finaliste à l'issue du troisième tour ;
- GeMSS (signature) – retenu comme alternatif à l'issue du troisième tour ;
- LAKE (mise en accord de clefs) ;

- LOCKER (chiffrement) ;
- SIKE (chiffrement, mise en accord de clefs) – retenu comme alternatif à l'issue du troisième tour ;

De plus, d'autres centres de recherche français, ne faisant pas partie du projet industriel RISQ, ont aussi participé à la compétition, seuls ou en collaboration avec des partenaires.

Implication des entreprises françaises

De nombreuses entreprises françaises travaillent sur le sujet de la cryptographie post quantique, que ce soit via (1) la participation à la compétition NIST, (2) le projet industriel RISQ, (3) des recherches autres, ou (4) au travers de partenariats tiers, comme par exemple Airbus, Crypto Expert, CS, Gemalto, Idemia, Secure IC, Thales, Orange, Worldline.

GLOSSAIRE

AES	Advanced Encryption Standard
DES	Data Encryption Standard
DH	Diffie Hellman
DSA	Digital Signature Algorithm
EC-DSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunication Standardisation Institute
HSM	Hardware Security Module
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Research Task Force
IKE	Internet Key Exchange
ISG	Industry Specification Group
ISO	International Organization for Standardization
LMS	Leighton-Micali Signature
NIST	National Institute of Standards and Technology
NSA	National Security Agency

PIA	Programme d'investissement d'avenir
PKI	Public Key Infrastructure
QSC	Quantum Safe Cryptography
RISQ	**R**egroupement de l'**I**ndustrie française pour la **S**écurité Post-**Q**uantique
RFC	Request For Comments
RSA	Rivest Shamir Adleman
SD	Standing Document
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TC	Technical Committee
TLS	Transport Layer Security
TR	Technical Report
WG	Working Group
XMSS	e**X**tended **M**erkle **S**ignature **S**cheme

Accréditations anonymes ou ABC (Attribute-Based Credentials)

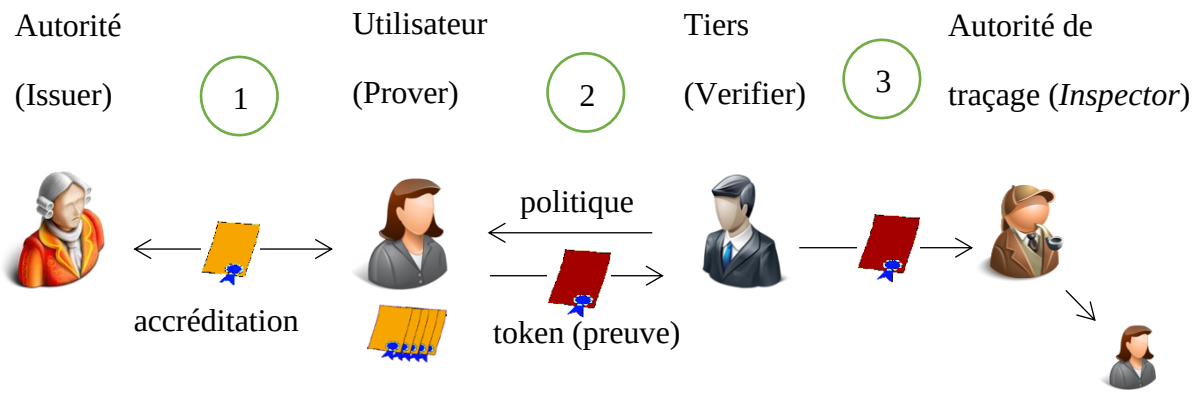
DESCRIPTION DE LA TECHNOLOGIE

La diversité terminologique « accréditations anonymes », « accréditations basées sur les attributs », « anonymous credentials », « ABC systems » ou « privacy-ABCs » désigne une même technologie de cryptographie. On utilisera ici le terme « d'accréditation anonyme ».

Les accréditations anonymes permettent de remplacer avantageusement les signatures numériques dans leur utilisation comme moyen d'authentification des personnes ou entités. Le problème des signatures numériques provient de ce qu'elles représentent un danger pour la vie privée du signataire. En effet, si l'on surveille un réseau de communication quelconque et que l'on voit passer ce qui ressemble à une signature émise par un inconnu, il suffira d'appliquer l'algorithme de vérification sur toutes les clés publiques à disposition pour déterminer à coup sûr l'identité de cet inconnu. On peut ainsi tracer les activités de tous les utilisateurs, avec même une valeur probante. Cet état de fait n'est pas compatible avec le principe du « privacy-by-design/default ».

Dans un système d'accréditation anonyme, au contraire, l'utilisateur va prouver à un tiers des vérités sur lui-même sans jamais révéler son identité complète. La quantité d'information capturée par le tiers est strictement minimisée au besoin du service qu'il opère et soumise au consentement de l'utilisateur. Ce changement de paradigme est en opposition forte avec la sur-identification largement répandue aujourd'hui qui peut conduire au vol de données personnelles et au vol d'identité.

Il existe 3 étapes essentielles dans le système, comme représenté sur la figure suivante.



Etape 1 (effectuée une fois pour toutes) : l'utilisateur obtient d'une autorité (ou Issuer) une accréditation sur ses attributs d'identité (nom, âge, genre, nationalité, statut étudiant, etc.). Cela suppose que l'autorité a validé les attributs par des moyens annexes, exactement comme une autorité de certification dans une infrastructure à clé publique. L'accréditation est un objet cryptographique assimilable à un certificat, et seule l'autorité dispose de la clé cryptographique maître permettant sa création. L'accréditation peut ensuite être utilisée à volonté par l'utilisateur.

Etape 2 (autant de fois que l'on veut) : pour accéder à un service, l'utilisateur va prouver à un tiers qu'il vérifie la politique d'accès (âge >= 18 et étudiant par exemple) sans rien révéler d'autre. Pour cela, il utilise son accréditation, la politique d'accès et un diversifiant de transaction émis par le tiers pour générer une donnée cryptographique randomisée appelée preuve de présentation ou « token ». Le tiers (ou Verifier) peut vérifier la validité du token ce qui, si le token est bien valide, prouve seulement que l'utilisateur dispose bien d'une accréditation sur un ensemble d'attributs inconnus qui vérifient la politique, mais aucune autre information ne peut en être soutirée. Le diversifiant de transaction garantit l'impossibilité d'un rejeu.

Etape 3 (optionnelle) : une autorité spéciale (Inspector) dispose d'une clé maître d'ouverture qui permet de déterminer l'identité complète de l'utilisateur qui a produit le token. L'existence de cette entité est optionnelle ; elle peut être utile en cas de dispute légale par exemple. L'ouverture de tokens permet de révoquer l'anonymat des utilisateurs et donc de revenir au niveau de traçabilité normal des signatures numériques (mais seulement pour l'autorité spéciale, les tokens restant parfaitement anonymes pour le reste du monde).

Il existe aujourd'hui des systèmes de contrôle d'accès avec anonymat partiel qui sont particulièrement répandus, comme OpenID Connect, SAML ou Facebook Connect. Bien que peu utilisés (ou même connus) en comparaison, les systèmes d'accréditations anonymes leur sont pourtant supérieurs à plusieurs titres :

- **Non-traçabilité plus forte** : sans même chercher à déterminer qui les a produits, juste déterminer si 2 tokens ont été produits par le même utilisateur ou par 2 utilisateurs différents est impossible (ceci n'est pas le cas avec OpenID Connect). Les transactions d'un utilisateur ne sont donc pas reliables entre elles à travers le temps ; on parle de « *unlinkability* », qui est le niveau maximal d'anonymat techniquement réalisable.

- **Résistance aux collusions contre les utilisateurs** : l'anonymat maximal est garanti même lorsque l'autorité est compromise, c'est-à-dire que la clé maître de production des accréditations est révélée à un attaquant.

- **Transactions hors ligne** : l'étape 2 (la transaction proprement dite) s'effectue seulement entre l'utilisateur et le tiers fournisseur de service.

Ceux-ci n'ont pas besoin d'entrer en contact avec l'autorité, contrairement à OpenID Connect qui impose à celle-ci de servir des requêtes http en temps réel. L'utilisateur peut ainsi être une carte à puce sans contact et le tiers une badgeuse à l'entrée d'un dispositif souterrain.

Enfin, certains systèmes d'accréditations anonymes bénéficient de mécanismes additionnels, comme la capacité d'agréger entre elles des accréditations provenant de plusieurs sources (comprendre : de plusieurs autorités), de décentraliser l'autorité au sein d'un groupe d'agents ou celle de fournir une preuve d'ouverture correcte par l'autorité spéciale.

On peut s'attendre à ce que ces systèmes, de par leur simplicité d'expérience et leurs garanties fortes de sécurité et d'anonymat, supplantent peu à peu les infrastructures actuelles en matière de fédération d'identité. Aujourd'hui, l'élément bloquant pour leur adoption généralisée par l'industrie est essentiellement l'absence de standard national, européen ou international.

MATURITE

Les premiers mécanismes dits de « anonymous credentials » remontent aux travaux de Chaum de 1985 qui prolongent son concept de signatures dites « aveugles » publié en 1982. Brands généralise ensuite ces techniques qui seront utilisées par sa startup Credentica pour concevoir le système U-Prove. Microsoft rachète cette société en 2008 et reformule U-Prove dans une spécification ouverte.

Ce champ de la cryptographie voit s'ouvrir une nouvelle branche entre 2001 et 2003 avec les signatures de Camenisch et Lysyanskaya, qui donneront naissance au système IdentityMixer ou « Idemix » d'IBM. Idemix et U-Prove, couverts par de nombreux brevets d'invention, ont fait l'objet d'une recherche d'interopérabilité et d'implémentations open-source efficaces dans le cadre du projet européen ABC4Trust. Il existe cependant des systèmes alternatifs dont les spécifications sont libres de tout droit de propriété intellectuelle, comme BBS+ ou IRMA et leurs variantes.

L'ensemble de ces solutions reposent sur des mécanismes cryptographiques bien connus (RSA, logarithme discret et courbes elliptiques avec ou sans couplage, preuves zero-knowledge) et disposent de preuves formelles de sécurité et d'anonymat. Comme tout autre mécanisme en cryptographie, leur implémentation comporte cependant des risques face aux attaques par canaux cachés et par injection de fautes, et peut donc nécessiter une évaluation de sécurité par un laboratoire indépendant avant tout déploiement.

Pour conclure, on peut considérer que la technologie ABC dispose d'un haut niveau de maturité sur le plan scientifique et technologique.

DEPLOIEMENTS/UTILISATION SUR LE TERRAIN

En contraste avec la maturité de cette technologie, les accréditations anonymes ne sont que peu employées par l'industrie mondiale de la sécurité. Cette frilosité s'explique par une triple conjonction : l'effet dissuasif des brevets de Microsoft et IBM, l'inertie importante des infrastructures actuellement déployées utilisant OpenID Connect ou assimilés, et le déficit en normalisation qui met en danger la pérennité d'investissements en matière de R&D.

Plusieurs applications pilotes ont cependant été mises au point et expérimentées sur des groupes restreints d'utilisateurs en Grèce et en Suède par des projets européens comme ABC4Trust et ReCRED, ou des universités telles que Radboud Universiteit aux Pays-Bas. Les pilotes ont démontré une grande facilité d'adoption renforcée par des expériences utilisateur particulièrement simples à la fois sur une application desktop, avec une carte à puce et sur un mobile Android. Le consentement de l'utilisateur requis lors de la production du token est perçu comme remettant l'utilisateur au cœur du système et la minimisation stricte des informations échangées rassure également le tiers fournisseur de service face à sa responsabilité en matière de traitement des données personnelles. Enfin, la non-implication de l'autorité dans les transactions locales simplifie considérablement le travail d'intégration des tiers développeurs et ouvre également la voie à des authentifications anonymes hors-ligne et en champ proche basées sur Bluetooth ou NFC.

CONTRAINTES

La contrainte la plus forte réside sur l'autorité émettrice d'accréditations, qui doit rester à la fois disponible et vigilante sur la validation des attributs à l'instar d'une autorité de certification dans une PKI. La concentration du risque est une caractéristique dont on peut souvent s'accommoder en pratique (après tout, les PKI actuellement utilisées pour les cartes bancaires et les passeports ne sont pas remises en cause sur le principe) mais qui motive la recherche de solutions alternatives décentralisées, par exemple à base de blockchain.

La révocation d'accréditations, c'est-à-dire l'annulation d'accréditations en cours d'utilisation sur le terrain, est aussi une contrainte complexe à prendre en compte opérationnellement. L'option la plus facilement réalisable consiste à ajouter une date d'expiration modérément proche (1 jour, 1 semaine, 1 mois, etc.) dans les attributs de l'accréditation, quitte à obliger les utilisateurs à se faire réémettre des accréditations plus souvent.

NORMALISATION

Si d'autres technologies d'authentification anonyme comme les signatures aveugles (ISO/IEC 18370) ou de groupe (ISO/IEC 20008 et 20009) font l'objet de normes internationales, et bien que les signatures en anneau et à seuil soient à

l'étude, aucune spécification de systèmes cryptographiques ABC n'est actuellement en cours de standardisation que ce soit à l'ISO, à l'ETSI, au W3C ou à l'IETF.

L'ISO SC 27 WG5 a cependant entrepris de normaliser des exigences de haut niveau portant sur l'ensemble des systèmes d'authentification à base d'attributs, qui incluent collectivement OpenID Connect, Sedicii, FIDO et les systèmes ABC. Il en ressortira que ceux-ci sont les seuls à réaliser le plus haut niveau d'exigence du fait de la propriété de « *unlinkability* ». La référence du standard en cours d'édition est ISO/IEC 27551 « Requirements for attribute-based unlinkable entity authentication ».

CAS D'USAGE IDENTIFIES

Tous les cas d'usage impliquant une authentification et une exigence de vie privée sont réalisables à l'aide d'accréditations anonymes. Suivent plusieurs exemples de contextes d'application :

- **Transports anonymes** : l'utilisateur achète un ticket (une accréditation) auprès du service de transport qui joue le rôle de l'autorité. L'accréditation est marquée par les attributs du ticket : date limite de validité, zones géographiques, ou statut particulier comme étudiant ou senior. L'accréditation est stockée dans une carte à puce ou une application mobile. Au moment de l'accès au transport, ou au moment d'un contrôle, le tourniquet (par exemple) défie l'utilisateur de prouver son droit d'accès, matérialisé par une politique (prédicat) sur les attributs et la date courante. La carte ou l'application mobile retourne une preuve de présentation randomisée et le tourniquet s'ouvre après vérification de ce token. La couche transport est assurée par l'interface NFC. L'utilisateur reste anonyme auprès du transporteur.

- **Paiements anonymes** : dans ce cas d'usage, l'autorité spéciale est nécessaire. L'utilisateur obtient une accréditation de sa banque qui certifie la validité d'un compte et éventuellement le droit à des tarifs particuliers. L'utilisateur paie anonymement en ligne avec son navigateur ou physiquement dans un magasin avec son mobile NFC en produisant un token marqué de la date et du coût de l'achat. Le token, une fois validé par le serveur ou la caisse, est remonté dans le back-end où il est ouvert par l'autorité spéciale pour pouvoir débiter le compte de l'utilisateur. L'utilisateur reste anonyme auprès du magasin tout en pouvant (potentiellement) prouver son droit à un tarif privilégié. Ce scenario est compatible avec la tokenisation EMV.

- **Contrôle d'accès physique** : une accréditation est obtenue d'un serveur d'entreprise et téléchargée dans un wallet applicatif sur un mobile compatible NFC. Le tiers vérifieur est un point de contrôle équipé d'un

lecteur NFC. Sur détection d'une présence en champ proche, celui-ci émet sa politique d'accès et un aléa (la politique peut typiquement dépendre de la plage horaire). L'application mobile retourne un token marqué par l'aléa qui prouve le droit d'accès. Après validation par le lecteur, le token est archivé dans un fichier de log et une autorité spéciale peut exister dans une infrastructure back-end pour la gestion d'incidents.

LICENCES ET BREVETS

Brevets couvrant Idemix (IBM) par date de priorité

- Non-transferable anonymous credentials. US7222362B1 Ran Canetti. 2000-05-15.
- Non-transferable anonymous credential system with optional anonymity revocation. US7360080B2 Jan Camenisch. 2000-11-03.
- Anonymous access to a service. US20040078475A1 Jan Camenisch. 2000-11-21.
- Non-transferable anonymous digital receipts. WO US CN JP KR US8788828B2 Elsie van Herrewegen. 2001-04-23.
- Revocation of anonymous certificates, credentials, and access rights. US US7543139B2 Jan Camenisch. 2001-12-21.
- Anonymous payment with a verification possibility by a defined party. US JP US20050010535A1 Jan Camenisch. 2002-05-30.
- Method and system for user attestation-signatures with attributes. WO EP US KR US20090049300A1 Jan Camenisch. 2003-10-17.
- Anonymity revocation. US US8122245B2 Jan Camenisch. 2004-05-28.
- Assertion message signatures. WO EP US CN JP KR TW US8341416B2 Jan Camenisch. 2006-05-21.
- Attestation of computing platforms. WO EP US CN JP US8555072B2 Jan Camenisch. 2006-08-31.
- Attributes in cryptographic credentials. US US8281131B2 Jan Camenisch. 2008-08-28.
- Forming Credentials. US20100063932A1 Jan Camenisch. 2008-09-08.
- Cryptographic proofs in data processing systems. US8527777B2 Jan Camenisch. 2010-07-30.
- Managing unlinkable identifiers for controlled privacy-friendly data exchange. US GB US20170104726A1 Jan Camenisch. 2014-05-13.
- Privacy-preserving attribute-based credentials. US10079686B2 Jan Camenisch. 2015-07-29.
- Credential-Based Authorization. US US20170359184A1 Jan Camenisch. 2016-06-09.

License IdentityMixer (IBM)

Un ensemble d'outils, incluant une librairie Java et un processeur XML développés par IBM, est mis en avant pour intégration dans des projets open-source. La licence associée est, au choix, une International License Agreement ou une licence Apache v.2. Cependant toute information partagée avec IBM devient de plein droit propriété d'IBM.

Brevets couvrant U-Prove (Microsoft) par date de priorité

- Preserving privacy with digital identities. US US9043891B2 Christian Paquin. 2010-02-18.
- Revoking delegatable anonymous credentials. US US8839381B2 Lan Nguyen. 2010-12-07.
- Adding privacy to standard credentials. WO EP US CN US20170163421A1 Melissa E. Chase. 2015-12-04.
- Minimal disclosure credential verification and revocation. WO EP US CN US9768962B2 Tolga Acar. 2013-03-15.

License U-Prove (Microsoft)

Microsoft a développé un SDK U-Prove sous licence open-source BSD. Les sources sont disponibles en C# ou Java et la technologie est couverte par un « Open Specification Promise », supposé protéger les projets intégrateurs de tout risque liés aux brevets. Il est cependant communément considéré douteux que la protection puisse légalement s'appliquer aux projets sous licence GPL et autres logiciels libres.

ACTEURS PROMOUVANT CETTE TECHNOLOGIE

- IBM (IBM Research, Zurich)
- Microsoft (Microsoft Research, US)
- AEvatar.coop (Paris, France)
- CryptoExperts (Paris, France)
- Radboud Universiteit (Pays-Bas)
- Hyperledger (Linux Foundation, International)
- ReCRED (Projet de recherche H2020)

Chiffrement homomorphe (ou FHE)

DESCRIPTION DE LA TECHNOLOGIE

Le chiffrement homomorphe (ou FHE pour *Fully Homomorphic Encryption*) est une boîte à outil cryptographique qui permet de chiffrer et de déchiffrer des données, et simultanément d'effectuer des calculs sur des données chiffrées sans avoir à les déchiffrer.

Cette technique particulière de chiffrement, aujourd'hui en plein essor scientifique et technologique, ouvre une voie révolutionnaire dans la résolution de nombreuses problématiques de sécurité et de vie privée.

Jusqu'en 2009, il était connu que certains mécanismes de chiffrement à clé publique (aujourd'hui appelés partiellement homomorphes) permettaient d'effectuer 1 seul type d'opération sur des données ; soit additionner ces données pour certains schémas, soit les multiplier pour d'autres. En 2009, Gentry (un cryptologue d'IBM) publie la première technique de chiffrement qui supporte simultanément l'addition et la multiplication de données chiffrées. Tout calcul pouvant se décomposer en ces 2 seules opérations, le schéma de Gentry est donc le premier capable d'instancier le paradigme du « crypto-calcul », dans lequel on peut exécuter toute fonction, même très complexe, sur des données chiffrées sans jamais avoir à les connaître. Cette découverte, surprenante pour beaucoup d'experts, met fin à 30 ans de spéculations sur l'existence même d'un tel mécanisme.

Mais le schéma de Gentry est inefficace : multiplier 2 bits entre eux prend 30 minutes et la taille de la clé est de l'ordre du teraoctet. L'annonce de ce résultat en 2009 s'accompagne donc d'un fort sentiment que celui-ci relève essentiellement d'un intérêt théorique. De nombreux travaux de recherche sont cependant entrepris dans la communauté cryptographique pour améliorer ces performances.

Une décennie plus tard, on constate que de nombreux autres schémas de chiffrement homomorphe ont vu le jour, et que leur efficacité est supérieure au schéma originel de Gentry de plusieurs (jusqu'à 5) ordres de grandeur. Plusieurs familles de constructions coexistent aujourd'hui, qu'il est d'usage de regrouper en « générations ».

Schémas de 1ère génération

Ils caractérisent les principes et techniques de base utilisées par Gentry et ses variantes :

- **Orientation binaire :** on ne peut chiffrer essentiellement que des bits individuels. Les données en clair sont donc décomposées en bits et le calcul est exprimé sous la forme d'un circuit booléen ;
- **Notion de bruit :** le chiffrement d'un bit nécessite l'insertion d'un aléa appelé « bruit » dans le chiffré (autrement il n'y a pas de sécurité) ;
- **Addition « facile » :** l'addition de 2 bits chiffrés est réalisée modulo 2, c'est-à-dire qu'on calcule le XOR de ces 2 bits. Cette opération, plutôt rapide comparativement à la multiplication, additionne les bruits des 2 chiffrés d'entrée de sorte que le bruit du chiffré de sortie soit en gros de la même taille ;
- **Multiplication « difficile » :** la multiplication de 2 bits chiffrés (c'est-à-dire leur ET logique) est cependant plus lente et qui plus est, agrège les bruits d'entrée de façon multiplicative de sorte que le bruit de sortie soit de taille double ;
- **Notion de « bootstrapping » :** la succession d'opérations homomorphes, additions et multiplications, provoque donc une amplification du bruit dans le circuit booléen jusqu'au point où le bruit dépasse une taille limite et « empiète » sur le message transporté. Le chiffré devient alors indéchiffrable. Gentry introduit donc une méthode dite de *bootstrapping* qui permet de convertir un chiffré très bruité en un nouveau chiffré peu bruité sans toutefois perturber le bit en clair sous-jacent. Une fois « nettoyé », le chiffré peut continuer à subir des opérations homomorphes jusqu'à ce qu'il soit de nouveau très bruité. On réapplique alors l'opération de *bootstrapping*, et ainsi de suite, jusqu'à calculer l'ensemble du circuit. On retourne ensuite les chiffrés de sortie au propriétaire des données qui peut les déchiffrer avec sa clé privée.

Si l'idée du *bootstrapping* est géniale, elle est néanmoins très coûteuse et rédhibitoire en pratique.

Schémas de 2nde génération

En 2012, plusieurs techniques nouvelles viennent changer ces contraintes quantitatives :

- **« Batching » :** on peut maintenant chiffrer des vecteurs de bits plutôt que des bits individuels, et sans réel surcoût dans la taille des chiffrés. Les opérations homomorphes opèrent sur chaque bit en parallèle, de sorte que l'on peut évaluer de multiples instances du même circuit booléen et ainsi rentabiliser l'ensemble du crypto-calcul effectué. Les chiffrés et les clés bénéficient aussi d'une réduction de taille importante.
- **Niveaux de bruit :** la méthode dite du « *modulus switching* » permet de fixer un nombre prédéterminé de niveaux de bruit distincts dans un chiffré, mettons de 1 jusqu'à une borne L.

- **Effet de l'addition :** si maintenant on effectue une addition homomorphe entre un chiffré de niveau i et un chiffré de niveau j (i,j dans {1, …, L}), le chiffré de sortie sera de niveau max(i, j).
- **Effet de la multiplication :** la multiplication retourne un chiffré de niveau max (i, j) + 1.

Ainsi, la taille du bruit grandit linéairement dans une succession de multiplications homomorphes, plutôt qu'exponentiellement comme dans les schémas de première génération, le gain étant très significatif. Lorsqu'on arrive au niveau L, on dispose également d'une opération de *bootstrapping* qui transforme un chiffré de niveau maximal L en un chiffré de niveau 1. On peut ainsi enchaîner les calculs à volonté. Le *bootstrapping* reste cependant l'opération la plus coûteuse à effectuer, et de loin.

La découverte de ces techniques (schémas BGV, FV, Brakerski, DGHV et leurs variantes) a stimulé l'émergence d'une double approche du paradigme du crypto-calcul :

- **L'approche « FHE »,** dans laquelle on utilise le *bootstrapping* comme une opération native chaque fois qu'on en a besoin pour évaluer l'intégralité du circuit. En cas de besoin, on pourrait même enchaîner avec d'autres calculs à l'issue.
- **L'approche « SHE »** (ou Somewhat Homomorphic Encryption), dans laquelle on ne souhaite pas ralentir les calculs avec des *bootstrappings*. On laisse le bruit grandir au fur et à mesure des opérations, mais on se débrouille pour fixer les paramètres du chiffrement de sorte à laisser un « réservoir de bruit » suffisant jusqu'à la fin du circuit. Les chiffrés de sortie ne peuvent subir aucun calcul ultérieur et ne peuvent qu'être retournés au propriétaire des résultats.

Schémas de 3ème génération

Un saut conceptuel est introduit avec le schéma GSW, qui simplifie beaucoup la compréhension du mécanisme de chiffrement et des opérations homomorphes. Malheureusement, cette simplification ne s'accompagne pas d'une amélioration (mais plutôt d'une détérioration) des performances. Les développeurs de librairies de crypto-calcul préféreront en majorité rester sur les schémas de seconde génération.

Schémas de 4ème génération

En 2016, une équipe mixte de chercheurs français issus du projet FUI de recherche Cryptocomp conçoit TFHE (Torus FHE), un schéma opérant sur des bits dans lequel le *bootstrapping* est extrêmement rapide et ne prend que quelques millisecondes sur un ordinateur grand public. Amélioré et étendu par la suite,

TFHE bénéficie à ce jour des chiffrés et des clés les plus compacts (quelques kilo-octets pour les chiffrés, quelques méga-octets pour la clé publique d'évaluation). TFHE introduit aussi une mesure différente de la complexité des crypto-calculs : si les schémas précédents cherchent à minimiser la profondeur multiplicative du circuit booléen à évaluer (son nombre maximal de multiplications successives), la complexité de TFHE dépend plutôt de la taille minimale d'un automate fini représentant la fonction à crypto-calculer. D'autres travaux accompagnant TFHE ont également permis de simplifier beaucoup le paramétrage de la sécurité du chiffrement, qui reste encore complexe pour les schémas de seconde génération.

Grâce à ces avancées, il est aujourd'hui admis par les experts que les performances du chiffrement homomorphe ne sont déjà plus un véritable problème pour une grande sous-classe de cas d'usage, et que l'effort de recherche doit maintenant s'intensifier, en parallèle des aspects cryptographiques, sur la disponibilité d'outils de compilation de qualité industrielle.

MATURITE

En ce début d'année 2019, le chiffrement homomorphe est caractérisé par des degrés de maturité variables selon les angles d'observation.

Aspects sur lesquels la technologie FHE est mature

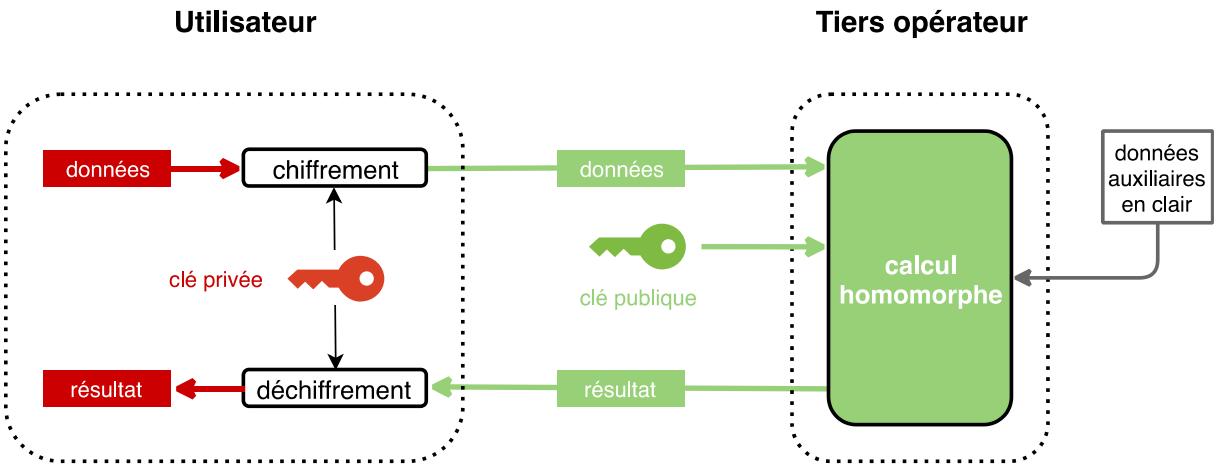
1. Après seulement une dizaine d'année de recherche internationale continue, devenue aujourd'hui très compétitive, l'état de l'art scientifique présente aujourd'hui une compréhension avancée des mécanismes cryptographiques de base qui sous-tendent le chiffrement homomorphe. Après une grande diversification exploratoire, ces dernières années ont vu s'opérer une convergence rapide des méthodes de conception, au point de partager aujourd'hui un vocabulaire commun et de susciter des initiatives de standardisation dans l'industrie.
2. La transformation générique d'un calcul « naïf » sur données en clair en un crypto-calcul équivalent sur données chiffrées est déjà maîtrisée sur le plan scientifique et commence à l'être aussi sur le plan technologique avec des outils de conversion automatique source-à-source tels que Cingulata, développé par le CEA. Ces outils compilent le code source du calcul « naïf » en synthétisant un circuit booléen (voire arithmétique) qui est ensuite instancié avec l'aide d'une API cryptographique universelle.
3. Un autre indicateur important de maturité réside dans l'utilisation des réseaux euclidiens et l'apport systématique par les concepteurs de preuves d'équivalence entre la sécurité de leurs schémas et des problèmes algorithmiques bien connus en réduction de réseaux. La métrique de sécurité pré-quantique est donc très bien maîtrisée, et les schémas de FHE sont par ailleurs de très bons candidats en matière de chiffrement résistant à l'ordinateur quantique.

Aspects sur lesquels la technologie FHE n'est pas mature

1. Le FHE présente un déficit de maturité en dehors du point 2 ci-dessus, c'est-à-dire pour réaliser des calculs spécifiques à certains algorithmes très précis, contrairement à un traitement générique souvent sous-optimal. La compétition internationale annuelle du workshop iDASH, qui confronte entre elles les meilleures équipes mondiales en FHE autour d'un cas d'usage de traitement homomorphe de données génomiques, montre bien les écarts énormes de performance mesurés entre l'approche générique automatisée (TFHE : 201 minutes) et le cas de schémas perfectionnés « à la main » spécifiquement pour le cas d'usage considéré (Duality : 0,09 minutes), qui s'avèrent plus efficaces de 3-4 ordres de grandeur. Une véritable compréhension de l'origine de ces écarts manque encore dans la production d'un outillage systématique.
2. La technologie manque de standards, pour des raisons expliquées plus loin.
3. Enfin, la sécurité post-quantique des problèmes liés à la réduction de réseaux reste largement inconnue. Un effort de recherche fondamentale est aujourd'hui nécessaire pour atteindre un consensus largement partagé sur cette question. Il se pourrait aussi que les réseaux particuliers (RLWE sur anneaux cyclotomiques) utilisés par la grande majorité des schémas de FHE pour accélérer leur performance prêtent le flanc à des attaques quantiques améliorées en regard du cas général.

CAS D'USAGE IDENTIFIES

Tous les cas d'usage relèvent du paradigme de « la délégation de calcul », dans lequel un utilisateur envoie à un tiers un ensemble de données chiffrées pour qu'un calcul soit effectué sur elles. Le tiers applique le calcul de façon homomorphe et renvoie le résultat chiffré à l'utilisateur qui le déchiffre avec sa propre clé, comme montré sur la figure suivante :



Ce contexte haut-niveau recouvre un grand nombre de cas d'usage simples et concrets :

- **Traitement de données de santé** : des données médicales (sensibles car soumises au code de santé publique) sont transmises chiffrées à un tiers pour extraction de statistiques, détection de risques particuliers ou formulation de données de remboursement. Un démonstrateur développé au CEA LIST montre l'efficacité d'un cas d'usage de cette nature où des statistiques sont extraites avec des temps de calculs homomorphes de l'ordre de la seconde.
- **Génomique personnelle :** le génome de l'utilisateur est fourni à un tiers sous la forme d'un fichier de SNPs chiffrés pour détection de risques pathologiques probables tel que le cancer du sein ou des maladies auto-immunes. Le tiers ne peut collecter les données génomiques. Circagene, une startup au Royaume-Uni, développe actuellement une marketplace de services d'analyse sur génome chiffré.
- **Analyses de données financières** : un portefeuille d'actifs est transmis chiffré à un tiers gestionnaire de patrimoine pour déterminer en homomorphe les meilleures positions d'achat ou de vente à mettre en œuvre.
- **Machine learning** : le tiers évalue un réseau de neurones homomorphiquement sur les données chiffrées de l'utilisateur et lui retourne le résultat de l'inférence. Ce cas d'usage est particulièrement recherché par l'industrie du machine learning et des offres commerciales sont actuellement en train de se positionner (Microsoft, Intel, CryptoExperts).
- **Publicité programmatique** : le ciblage publicitaire s'opère en homomorphe ; match entre un profil de consommateur chiffré et une cible recherchée par un réseau d'annonceurs. La startup française Ravel développe actuellement une offre technologique.
- **Base de données chiffrées** : version homomorphe de SQL opérant sur une base de données chiffrée ou partiellement chiffrée. Ce cas d'usage très vaste et prometteur n'est pas résolu de façon satisfaisante aujourd'hui.
- **Economies d'énergie** : les données de consommation d'un compteur intelligent sont remontées chiffrées à un fournisseur de service dans le nuage pour recommander l'opérateur d'énergie le plus adapté, potentiellement en temps réel.
- **Smart contracts** : le contrat est chiffré et exécuté homomorphiquement par une blockchain intelligente de type Ethereum, ce qui permet de conserver la confidentialité du contrat. La startup NuCypher développe actuellement une offre sur la base de sa librairie libre nuFHE.

Plusieurs solutions commerciales sont aujourd'hui disponibles auprès de startups telles que Duality (US), Enveil (US), Galois (US), Cosmian (FR) ou CryptoExperts

(FR). Ce sont des offres d'intégration d'outils logiciels sous licence assorties d'un accompagnement en conseil.

CONTRAINTES

Dans l'état actuel des connaissances, on ne peut agréger des données chiffrées sous des clés d'utilisateurs différents sans implications indésirables sur le modèle de sécurité. Les différentes approches exploratoires dites de FHE « multi-clé » ne satisfont pas les fonctionnalités qu'on attendrait d'un tel concept. Jusqu'à nouvel ordre, l'utilisation du chiffrement homomorphe implique une « étanchéité » entre les données des utilisateurs.

Les contraintes les plus fortes proviennent des latences très variables de l'étape de crypto-calcul, et qui dépendent à la fois du mécanisme cryptographique choisi, des particularités de l'algorithme visé, de l'architecture hardware et du format choisi pour représenter les données. L'optimisation simultanée de tous ces paramètres tient actuellement plus de la créativité humaine que de quoi que ce soit d'autre, avec des résultats très variables et difficilement prédictibles.

NORMALISATION

Le chiffrement homomorphe est en cours de normalisation à l'ISO SC 27. La norme ISO/IEC 18033-6 « Homomorphic Encryption », dont la première édition sera publiée courant 2019, contiendra les schémas de El Gamal et de Paillier qui ne sont que partiellement homomorphes. A ce stade, l'ISO ne considère pas les techniques actuelles de FHE comme étant suffisamment matures pour une standardisation. Cette position pourra être réactualisée dans les années à venir.

Indépendamment des organisations traditionnelles de normalisation, un consortium industriel initialement formé par Microsoft Research et quelques startups américaines et européennes (mais dont les rangs ne cessent de grossir, voir http://homomorphicencryption.org), a pris l'initiative de produire un « standard de fait » pour fédérer les solutions industrielles de FHE. La cible du futur standard n'est pas de couvrir les techniques cryptographiques proprement dites, mais de concevoir une API universelle crypto-agnostique destinée aux développeurs de compilateurs homomorphes et qui leur permet d'être comparables et interopérables.

LICENCES ET BREVETS

Un grand nombre de librairies open-source de chiffrement homomorphe sont disponibles :

- SEAL (Microsoft) sous licence MIT
- HELib (IBM) sous license Apache v2

- PALISADE (Duality) sous copyright du New Jersey Institute of Technology
- NFLLib et FV-NFLlib (CryptoExperts, Quarkslabs) sous license GPLv3
- Cingulata (CEA List) sous license CeCILL-C
- cuFHE (VernamLab) sous license MIT
- Heaan (Seoul University) sous license Creative Commons
- nuFHE (NuCypher) sous license GPLv3
- TFHE (Cryptocomp team) sous license Apache v2

Une guerre de brevets a actuellement lieu autour du chiffrement homomorphe. Google Patents recense plus de 2200 brevets ayant trait au sujet. Il faut cependant noter l'importance de séparer les brevets portant sur des méthodes de conception cryptographique et les brevets d'application sensiblement plus nombreux.

ACTEURS PROMOUVANT CETTE TECHNOLOGIE

Grands industriels

IBM, Intel, Microsoft, SAP, Bertin, Gemalto, ViAccess, Orange Labs, Thales, NXP

Startups

Inpher (CH), Duality (US), Enveil (US), Cosmian (FR), Circagene (UK), CryptoExperts (FR), Galois (US), Ravel (FR), nuCypher (US).

Recherche académique

CEA (FR), Ecole Normale Supérieure, INRIA. **Universités** : MIT, Cincinnati, Brown, Hannover, Toronto, Waterloo, Sabanci, Seoul, Worcester Polytechnic Institute, EPFL, NJIT, UCSD, Versailles-Saint-Quentin,

Agences gouvernementales

NIH, NIST, NSF, SPAWAR, DARPA, IARPA

Chiffrement basé sur l'identité et sur les attributs (IBE, ABE)

CONCEPTS SOUS-JACENTS

Chiffrement basé sur l'identité (*Identity-Based Encryption*)

Le concept de l'IBE a été introduit en 1984, par Adi Shamir (l'un des co-inventeurs du RSA), qui a imaginé utiliser n'importe quelle chaîne de caractères (adresse courriel ou téléphone) comme clé publique de chiffrement, au lieu d'un objet mathématique au format particulier.

Puisque l'on connaît a priori la véracité de (par exemple) l'adresse courriel du destinataire du message, il est inutile d'exiger un certificat numérique sur elle, ce qui élimine la complexité liée à l'utilisation d'une infrastructure à clef publique. Cette méthode évite d'avoir à générer ou vérifier des certificats et le chiffrement IBE assure ainsi des étapes de préparation quasi-inexistantes pour les utilisateurs.

En revanche, une fois le message chiffré sous l'adresse courriel, le destinataire doit se faire remettre une clé de déchiffrement correspondant à cette adresse. La création de cette clé utilisateur est assurée par une autorité dédiée à cette tâche et doté d'une clé maître spéciale. La remise au destinataire de sa clé de déchiffrement est faite une fois pour toute, quitte à renouveler l'opération pour une nouvelle identité. L'adresse courriel est un exemple typique, mais l'adresse IP ou MAC d'un dispositif connecté, et plus généralement toute chaîne de caractère, est également utilisable en pratique.

Les premières solutions de chiffrement basée sur l'identité ont été découvertes en 2001, avec le cryptosystème de Boneh et Franklin (basé sur le couplage de Weil sur courbes elliptiques) et celui de Cocks (basé sur les résidus quadratiques). D'autres mécanismes ont rapidement suivi basés sur les différentes variantes du problème algorithmique dit du Diffie-Hellman bilinéaire. De nombreuses recherches académiques se sont poursuivies sur ce sujet jusque vers 2010.

Quelques produits et solutions commerciaux sont aujourd'hui disponibles, utilisés notamment pour le chiffrement de courriels (par exemple la société britannique Microfocus, repreneur de HPE logiciels, lui-même repreneur de la société américaine Voltage Security).

Avantages et inconvénients de l'IBE

L'IBE est séduisant en pratique du fait des avantages suivants :

- Absence de préparation pour le destinataire du message (création de la clé du destinataire « juste avant l'usage »).
- Pas d'infrastructure à clé publique requise pour les utilisateurs, permettant un client léger.

En revanche, cette technologie comporte aussi des inconvénients :

- La clé maître de l'autorité est fortement critique. Celui qui en dispose peut recréer des clés de déchiffrement à volonté sur toute identité, et donc déchiffrer la totalité des flux des utilisateurs. Cette centralisation fait porter un risque de sécurité informatique majeur au système. Il est partiellement mitigé dans les structures hiérarchiques (on parle alors de HIBE) qui permettent de déléguer les décisions par sous périmètre, mais jamais complètement.
- Dans ce contexte, les utilisateurs du système doivent donc accepter l'existence d'un « passe » étendu détenu par l'autorité et que leurs messages ne sont pas confidentiels vis-à-vis d'elle.
- Enfin, la révocation d'une clé de déchiffrement utilisateur n'est pas assurée. En pratique, on résout ce problème par un horodatage des identités.

Comme on le voit, l'IBE est une solution de chiffrement qui est plus facile à mettre en œuvre et sans doute plus facile à utiliser pour des utilisateurs inexpérimentés mais aussi plus délicate en termes de garanties de sécurité et de vie privée.

Généralement elle est utilisée pour chiffrer des mails dans un esprit plutôt de garantie de moyens que de garantie de résultats. L'Estonie l'a utilisée avec S/MIME (utilisation de l'adresse courriel officielle estonienne). L'IBE est aussi utilisé parfois pour l'accès au Cloud ou pour des paiements.

Chiffrement basé sur les attributs (*Attribute-Based Encryption*)

Le chiffrement à base d'attributs (Attribute-Based Encryption) est une approche relativement récente, décrite pour la première fois par Amit Sahai et Brent Waters en 2004[42], qui généralise le concept de chiffrement basé sur l'identité.

Lorsqu'il est nécessaire de fournir un accès à des données à de nombreux utilisateurs, IBE est inefficace, car il est nécessaire que ces données soient rechiffrées séparément avec l'identité de chaque utilisateur. Le chiffrement ABE apporte une solution efficace à ce problème.

[42] Amit Sahai and Brent Waters, Fuzzy Identity-Based Encryption Cryptology ePrint Archive, Report 2004/086 (2004)

Attributs et politiques

Le système peut prévoir plusieurs catégories d'attributs :

- Attributs de ressources : Type, Créateur, Prénom, ...
- Les attributs du sujet : Prénom, Département, Position, ...
- Actions d'attributs : Prénom, ...
- Environnement d'attributs : adresse IP, Temps, Dispositif, ...

Simultanément, on peut formuler des politiques (*policies*) sur des attributs. Une politique est une suite de conditions portant sur la valeur des attributs combinées par des opérations logiques « Et » et « Ou ». Un ensemble d'attributs donné peut satisfaire ou ne pas satisfaire une politique donnée.

Le concept du chiffrement ABE

Dans un chiffrement ABE :

- Les données sont chiffrées en y incorporant un ensemble d'attributs arbitraires. Le chiffré est donc marqué par les attributs choisis au moment du chiffrement.
- Pour pouvoir déchiffrer, un utilisateur se fait remettre de l'autorité une clé de déchiffrement qui incorpore une politique choisie par l'autorité. L'autorité dispose d'une clé maître permettant la création à volonté de clés de déchiffrement utilisateur.
- La procédure de déchiffrement ne fonctionne que si l'ensemble des attributs du chiffré satisfait la politique de la clé de déchiffrement (sinon, la procédure retourne une erreur).

ABE permet de n'autoriser quelqu'un à déchiffrer un message que s'il détient une clé pour les « attributs correspondants », les clés utilisateur étant toujours émises par l'autorité, qui est une partie de confiance. Dans ce modèle, la complexité de la politique n'est pas limitée.

La stratégie de contrôle d'accès peut s'exercer sur les objets à protéger (par exemple, des fichiers, pour lesquels des attributs et une politique d'accès sont définis) ou sur les clés cryptographiques via lesquelles l'accès est effectué (ici, la clé ne fonctionne que lorsque les attributs du message chiffré répondent à la stratégie). Pour calculer les autorisations, tous les attributs sont lus au moment de la détermination des droits de contrôle et comparés aux valeurs attendues. Le respect de toutes les conditions donne accès à une ressource.

Ciphertext-Policy ABE et Key-Policy ABE

Si on le souhaite, on peut inverser les rôles de l'ensemble d'attributs et de la politique d'accès. Le chiffré est alors marqué par la politique au moment du

chiffrement, et l'ensemble d'attributs est appliqué à la clé de déchiffrement remise à un utilisateur. Là encore, le déchiffrement ne fonctionne que si l'ensemble des attributs de la clé satisfait la politique du chiffré.

Ces 2 variantes d'ABE sont appelées

- Ciphertext-Policy ABE (ou CP-ABE) lorsque la politique est intégrée au chiffré, ou
- Key-Policy ABE (ou KP-ABE) lorsqu'elle est intégrée à la clé de déchiffrement.

Cas d'usage CP-ABE

Dans le chiffrement CP-ABE, une clé privée d'utilisateur est associée à un ensemble d'attributs et un cryptogramme n'est exploitable que par un récipiendaire satisfaisant une stratégie d'accès sur un univers défini d'attributs. Un utilisateur pourra alors déchiffrer un texte chiffré si et seulement si ses attributs satisfont à la politique associée au texte chiffré reçu. Les stratégies

Les politiques peuvent être définies sur des attributs en utilisant des conjonctions, des disjonctions et des seuils (k, n), c'est-à-dire que k sur n attributs doivent être présents (il peut également y avoir des stratégies d'accès complexes, spécifiant notamment des négations supplémentaires ou des circuits arbitraires).

Par exemple, supposons que l'univers d'attributs soit défini comme étant {A, B, C, D} et que l'utilisateur 1 reçoive une clé pour les attributs {A, B} et l'utilisateur 2 une clé pour l'attribut {D}. Si un texte est chiffré par rapport à la politique *(A et C) ou D*, l'utilisateur 2 pourra alors le déchiffrer, tandis que l'utilisateur 1 ne le pourra pas.

Utilisateur	**A**	**B**	**C**	**D**
Condition	(A ET C) OU D			
User 1	X	X		
User 2				X

Tableau 1 - Politique (A ET C) OU D

CP-ABE permet ainsi de réaliser une autorisation implicite, c'est-à-dire qu'une autorisation est incluse dans les données chiffrées si bien que seules les personnes satisfaisant à la politique associée peuvent déchiffrer les données. Un aspect intéressant est que les utilisateurs peuvent obtenir leurs clés privées une fois que les données ont été chiffrées conformément aux stratégies. Ainsi, les données peuvent être chiffrées sans connaître le groupe d'utilisateurs pouvant déchiffrer, mais uniquement la stratégie permettant de déchiffrer. Tous les futurs utilisateurs auxquels une clé relative à ces attributs sera attribuée seront alors en mesure de

déchiffrer les données. Dans cette approche, il est alors possible de limiter les entités ayant accès à une information.

Cas d'usage KP-ABE

KP-ABE est le pendant de CP-ABE en ce sens qu'une politique d'accès est contenue dans la clé privée de déchiffrement de l'utilisateur, par exemple *(A ou C) ou D*, et qu'un texte chiffré est calculé par rapport à un ensemble d'attributs, par exemple, {A, B}. Ici, l'utilisateur ne pourrait pas déchiffrer le texte chiffré, mais pourrait par exemple déchiffrer un texte chiffré par rapport à {A, C}.

Utilisateur	**A**	**B**	**C**	**D**
Condition	Chiffrement {A, C}			
User 1	X	X		
User 2				X

Dans cette approche, il est alors possible de définir des groupes d'entités avec des droits définis.

Contraintes

Bien que le concept d'ABE soit très puissant et prometteur, ces systèmes souffrent principalement de deux inconvénients : la non-efficacité et la non-existence d'un mécanisme standard de révocation d'attribut d'un utilisateur.

Les autres principaux défis sont :

- La coordination des clés : comment effectuer la mise à jour des clés lorsqu'un attribut évolue ? Comment gérer la création et la distribution des clés lorsque les attributs sont sous la responsabilité de plusieurs entités différentes ?
- Le séquestre des clés, qui doit être séparé de la gestion des attributs
- La révocation des clés

Mécanisme de révocation d'attribut

La révocation des utilisateurs dans les systèmes cryptographiques est un problème bien étudié mais non trivial. La révocation est encore plus difficile dans les systèmes à base d'attributs, étant donné que chaque attribut appartient éventuellement à plusieurs utilisateurs différents, alors que dans les systèmes PKI traditionnels, les paires de clés publique / privée sont associées de manière unique à un seul utilisateur. En principe, dans un système ABE, les attributs, et non les utilisateurs ou les clés, peuvent être révoqués.

Une solution simple mais contrainte pour implémenter la révocation consiste à inclure un attribut temporel. La valeur de l'attribut temporel sera ainsi vérifiée par rapport à la politique de contrôle d'accès définie pour le cryptogramme (ex. T < 20181231).

Par exemple, ce peut être l'attribut « date » dont la valeur change une fois par jour. On suppose que chaque utilisateur non révoqué reçoit ses nouvelles clés privées correspondant à l'attribut « date » une fois par jour, directement du serveur principal (MKS, Mobile Key Server, qui est l'autorité centrale) ou par l'intermédiaire des serveurs délégués régionaux.

Par ailleurs, avec une structure d'accès hiérarchique, la propriété de délégation de clé de CP-ABE peut être exploitée pour réduire la dépendance vis-à-vis de l'autorité centrale pour l'émission des nouvelles clés privées à tous les utilisateurs à chaque intervalle de temps. Il existe des compromis importants entre la charge supplémentaire supportée par l'autorité pour générer et communiquer les nouvelles clés aux utilisateurs et le temps qui peut s'écouler avant qu'un utilisateur révoqué puisse être efficacement purgé.

La solution ci-dessus a les problèmes suivants :

- Chaque utilisateur X doit recevoir périodiquement de l'autorité centrale la nouvelle clé privée correspondant à l'attribut time, sinon X ne pourra déchiffrer aucun message.
- Il s'agit d'une technique de révocation simple par laquelle l'utilisateur révoqué n'est pas purgé du système avant l'expiration de la période actuelle.
- Ce schéma nécessite une synchronisation implicite de l'heure (une synchronisation lâche peut être suffisante) entre l'autorité et les utilisateurs.

RESISTANCE AUX ATTAQUES

Sur le plan mathématique, les mécanismes IBE matures et standardisés utilisent un objet mathématique appelé couplage sur courbe elliptique. Leur sécurité dépend donc de la capacité à choisir des courbes suffisamment sûres, au sens ou certaines opérations de calcul sur ces courbes (qui permettraient une attaque) ne soient pas réalisables même avec un effort de calcul très important (calcul classique non quantique). La maîtrise de ces conditions est scientifiquement acquise, avec cependant des avancées scientifiques sporadiques qui imposent de réviser toutes les quelques années le choix des bonnes courbes à utiliser.

En revanche, la sécurité des courbes elliptiques (avec ou sans couplage) s'effondre totalement en présence d'un ordinateur quantique. Dans ce cas, il est possible d'utiliser des mécanismes IBE alternatifs qui se basent sur des réseaux euclidiens en lieu et place des couplages sur courbes elliptiques. De tels mécanismes sont connus dans la littérature cryptographique mais ne sont actuellement pas

standardisés ou utilisés, et occasionnent un accroissement de la taille des clés et des chiffrés, ainsi qu'un surcoût de temps d'exécution. La sécurité post-quantique des réseaux euclidiens reste une question ouverte à ce jour, mais elle a le bon goût de ne pas s'effondrer trivialement comme celle des courbes elliptiques.

Sur le plan structurel, la technologie IBE implique un niveau de confiance élevé dans le tiers générateur des clés privées associées aux clés publiques distribuées ; ce tiers sera vraisemblablement la cible première de tout attaquant et sa sécurité, essentiellement basée sur un renouvellement régulier de la clé mère, induit une contrainte sur les processus de gestion des clés. La fonction « oracle » exposée par ce tiers, qui permet l'extraction d'une clé secrète associée à une identité *id*, ouvre une faille dans le cryptosystème en permettant à l'attaquant de cibler une *id* particulière.

Pour ABE, une propriété importante qui doit être atteinte à la fois par CP- et KP-ABE est la « résistance à la collusion ». Cette propriété interdit à des utilisateurs distincts de « mettre en commun » leurs clés privées de manière à pouvoir déchiffrer ensemble un texte crypté qu'aucun d'entre eux ne pourrait déchiffrer par lui-même (ce qui est obtenu en brouillant aléatoirement et indépendamment les clés privées des utilisateurs). Par exemple, pour le message envoyé avec la politique *(A et C) ou D*, un utilisateur possédant l'attribut A et un utilisateur possédant l'attribut C ne peuvent pas mettre en commun leurs informations pour déchiffrer le message.

MATURITE

La technologie IBE est bien comprise, avec une présence importante en standardisation et des librairies open-source disponibles. Naturellement, le paradigme émergent du calcul quantique remet en question ce haut degré de maturité, mais cela est vrai pour un grand nombre de mécanismes cryptographiques et n'est pas propre à IBE.

Une rapide recherche de publications consacrées à la technologie IBE fait apparaitre plus de 33000 résultats, les plus récentes abordant presque toutes les problématiques liées au stockage en nuage.

Beaucoup de publications de recherche sur ABE (17000+ résultats retournés par Google Scholar) sont également accessibles, mais aucun produit ou solution ne fait explicitement référence à cette technologie.

Déploiements/utilisation sur le terrain

La technologie IBE est au cœur de quelques études portant sur des mécanismes de protection des contenus déposés sur les réseaux sociaux, afin d'améliorer le niveau de protection de la vie privée des adhérents. Cette technologie reste

néanmoins largement proposée pour assurer la sécurité des espaces de stockage offerts par les grands fournisseurs du cloud ou le chiffrement de mails.

Le chiffrement par attributs est une technologie récente et n'est pas encore largement répandue, mais de nombreuses applications sont possibles. Il peut être utilisé pour le chiffrement des journaux systèmes : au lieu de chiffrer un message pour chaque destinataire, le message est chiffré avec certains attributs ce qui réduit la quantité de clés à utiliser. Le chiffrement par attributs est aussi utile dans un contexte pair-à-pair où il n'y a pas de serveur central pour gérer les politiques d'accès.

CAS D'USAGE IDENTIFIES

Comme vu plus haut, la majorité des applications pouvant mettre en œuvre la technologie IBE mettent en œuvre un tiers de confiance :

- Chiffrement de courriels, où elle est particulièrement simple à déployer.
- Stockage dans le nuage : le fournisseur de la solution de stockage gère l'attribution des clés, liées à l'identité des possesseurs de comptes. Un cas dérivé est celui de la protection des échanges au sein d'un réseau d'objets intelligents (IoT ou *Wireless Sensor Networks*).
- Protection des contenus sur les réseaux sociaux
- Sécurisation des transactions électroniques multipartites : ex. transaction de paiement en e-commerce, où le tiers de confiance peut être une entité interfaçant le marchand et la banque du consommateur

La technologie ABE est adaptée à différentes applications, selon le mode de chiffrement retenu :

- Mode *Content-based Access Control* : la clé dépend d'attributs liés au message lui-même (i.e. « To:rh@company.com »)
- Mode *Role-based Access Control* : la clé dépend du rôle du destinataire (i.e. l'accès à un dossier médical est réservé à un médecin).

On peut citer, de façon non-exhaustive :

- Chiffrement de contenus (mails ou documents) au cours de leur transmission ou de leur stockage : santé, militaire, réseaux sociaux, …
- Contrôle d'accès logique : réseau, applications d'entreprise, ressources cloud
- Contrôle d'accès physique : industries sensibles (OIV), militaire
- Validation d'attributs : certification de l'âge du porteur pour des applications gouvernementales, des restrictions de distribution (i.e. alcool, tabac), des applications financières (ouverture d'un dossier de crédit), etc.

NORMALISATION

Pour IBE, le lecteur peut trouver la base normative dans les documents suivants :

- IETF 5091 "Supersingular Curve Implementations of the BF and BB1 Cryptosystems."
- IETC 5408 "Identity-Based Encryption Architecture and Supporting Data Structures."
- IETF 5409 "Using the Boneh-Franklin and Boneh-Boyen Identity-Based Encryption Algorithms with the Cryptographic Message Syntax (CMS)."
- IEEE 1363.3 "IEEE Standard for Identity-Based Cryptographic Techniques using Pairings".
- ISO 15946-1 "Pairings Based Crypto (2008)."

La technologie ABE s'appuie essentiellement sur les standards régissant les échanges cryptographiques. Plusieurs groupes de travail à l'ETSI, à l'ISO ou au NIST ont consacré des publications, à caractère de recommandation ou de spécification :

- OASIS Security Assertion Markup Language (SAML) V2.0 (http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip)
- OASIS XACML (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)
- ETSI : TS 103 532 V1.1.1 (2018-03) "Attribute Based Encryption for Attribute Based Access Control"[43], TS 103 458 "Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements"[44]
- ISO/IEC SC 27, Working Group 2 - Cryptography and security mechanisms
- 3GPP TR22.891 "Study on New Services and Markets Technology Enablers" (https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2897)
- NIST "Guide to Attribute Based Access Control (ABAC) Definition and Considerations" (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-162.pdf)

LICENCES ET BREVETS

La technologie IBE est notamment à la base des brevets :

- 2006- 7113594 B2 -SYSTEMS AND METHODS FOR IDENTITY-BASED ENCRYPTION AND RELATED CRYPTOGRAPHIC TECHNIQUES

[43] https://www.etsi.org/deliver/etsi_ts/103500_103599/103532/01.01.01_60/ts_103532v010101p.pdf
[44] https://www.etsi.org/deliver/etsi_ts/103400_103499/103458/01.01.01_60/ts_103458v010101p.pdf

- 2006- 7003117 B2 -IDENTITY-BASED ENCRYPTION SYSTEM FOR SECURE DATA DISTRIBUTION
- 2012- 8320559 B1 - IDENTITY BASED ENCRYPTION SYSTEM
- 2014 – 8627103 B2 IDENTITY BASED ENCRYPTION OF DATA ITEMS FOR SECURE ACCESS
- 2016 – 9356779 B2 SYSTEMS AND METHODS FOR IBE AND RELATED CRYPTOGRAPHIC TECHNIQUES

Pour ABE, le lecteur consultera avec intérêt les brevets :

- Zeutro : multi-authority ABE (Zeutro's US Patent No. 8516244), ABE keystore (Zeutro's US Patent No. 9209974)
- US 20140129845A1 "Attribute based encryption using lattices" (Microsoft Technology Licensing LLC)
- US 20150222605A1 "Attribute-based encryption" (Koninklijke Philips NV)
- US 20160241399A1 "Efficient Privacy-Preserving Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption" (Arizona State University)

ACTEURS PROMOUVANT CES TECHNOLOGIES

La société américaine Voltage Security a été la première à proposer une offre logicielle IBE et à contribuer à produire le premier standard d'IBE au sein du IEEE. D'autres offres commerciales sont disponibles, comme celle de Fortinet.

Zeutro : https://www.zeutro.com/technology.html, fournit une librairie open source C++ (OpenABE) permettant d'implémenter la technologie au sein de toute application.

Les acteurs principaux œuvrant autour de la technologie sont essentiellement des équipes de recherche universitaires, de petites structures de développement ou de conseil sur les technologies et bien évidemment les grandes sociétés dans le domaine de la sécurité.

Conclusion

De nombreuses techniques cryptographiques permettent d'apporter des réponses nouvelles aux besoins grandissant qui sont :

- La non traçabilité et techniques d'anonymisation ;
- La protection des données personnelles ;
- Le contrôle et la souveraineté des données, lors du stockage et du traitement des données en nuage ;
- La résilience contre les cyberattaques et la sécurité à long terme ;
- La sécurité numérique et le nomadisme technologique ;

BLOCKCHAIN

Cette technologie est globalement mature et recommandée. Elle est devenue à présent très populaire, et des utilisations réelles émergent chaque jour (banque, finance, énergie, traçabilité de produits…). Cette technologie est globalement mature, sauf peut-être les aspects liés aux algorithmes de consensus qui doivent encore faire l'objet de travaux académiques.

Cette technologie est toutefois suffisamment performante pour pouvoir être mise en œuvre dès à présent dans le domaine de l'identité numérique. Elle permettrait entre autres de mettre en place des bases de données décentralisées, contrôlées non pas par une autorité centrale unique, mais plutôt par un réseau d'autorités de confiance décentralisé. Ainsi, elle permettrait de réaliser :

- Des **émissions décentralisées** d'identité numérique par des autorités elles-mêmes décentralisées (par exemple mairie ou préfecture) ;
- Des **révocations décentralisées** d'identités numériques par des autorités elles-mêmes décentralisées (par exemple des mairies ou préfectures) ;
- Des **gestions et mises à jour décentralisées de données** (par exemple des attributs d'identité mis à jour par un tiers ou le porteur lui-même).

De plus, cette technologie permet de garder une traçabilité des différentes actions tout en préservant l'anonymat de son acteur.

Même si en termes techniques, cette technologie est mature et prête à être utilisée, elle manque aujourd'hui d'un cadre règlementaire et légal (même si plusieurs efforts sont en cours). Ceci peut bloquer l'intégration de cette technologie dans certains domaines où l'existence d'une législation adéquate est obligatoire.

Enfin cette technologie est peu concernée par le risque de l'ordinateur quantique.

CRYPTOGRAPHIE EN BOITE BLANCHE

Cette technologie est mature. Elle permet (1) de mettre en œuvre des mécanismes cryptographiques et (2) de protéger, avec un relatif niveau de confiance, les clefs cryptographiques dans un dispositif n'utilisant pas d'éléments sécurisés (par exemple téléphone, tablette…). Cette technologie est devenue très populaire au cours des dernières années, notamment grâce aux solutions proposant de virtualiser une carte bancaire dans un téléphone mobile ne possédant pas d'éléments sécurisés (HCE – Host Card Emulation). Cependant, il est important de la combiner à d'autres techniques de protection logicielle (comme l'obfuscation), afin de fournir une protection en couches, plus difficile à casser. Ces différentes techniques sont décrites dans le rapport technique TR 103 642 préparé par l'ETSI.

Toutefois, il faut bien garder à l'esprit que cette technologie ne permet pas d'offrir un niveau de protection des clefs cryptographiques comparable à celui offert par un élément sécurisé matériel. Il s'agit plutôt d'une alternative par défaut. En effet, les clefs cryptographiques peuvent être retrouvées par un attaquant procédant à une analyse ou une rétroconception du code exécutable dans lequel elles sont dissimulées. Cette technologie permet toutefois de sécuriser des applications mobiles où l'accès à des éléments matériels sécurisés (de type µSD, élément sécurisé...) est difficile voire impossible.

Plus généralement, ces technologies de protection logicielles ne représentent qu'une partie de la sécurité globale d'un service, qui doit aussi être complétée par (1) des mesures de sécurisation du serveur central, interagissant avec le logiciel s'exécutant sur le dispositif, (2) une détection de fraude sur le serveur central permettant de détecter des comportements anormaux des dispositifs pouvant traduire une corruption des clefs cryptographiques, et (3) d'une gestion de risque. En effet, l'opérateur du service doit assumer et gérer le risque global découlant de cette technologie.

CRYPTOGRAPHIE « ZERO KNOWLEDGE »

Cette technologie est mature et recommandée. Elle permet de prouver des attributs à un tiers, sans les lui divulguer.

Elle peut dès à présent être mise en œuvre dans le cadre d'un service d'identité numérique, pour permettre à un porteur de prouver des attributs d'identité (majorité, adresse…) sans les divulguer. En cela, cette technologie permet de renforcer la protection des données personnelles et l'anonymat des individus.

Toutefois, cette technologie ne permet pas à elle seule de garantir la protection des données personnelles ou l'anonymat d'un porteur. L'appréciation globale d'un service utilisant cette technologie en termes de protection des données personnelles et d'anonymat du porteur doit être faite au cas par cas.

Enfin, bien que cette technologie soit aussi concernée par le risque de l'ordinateur quantique, et qu'une nouvelle génération résistante à l'ordinateur quantique reste encore à inventer, cela ne remet pas forcément en cause sa pertinence. Les preuves d'attributs créées par cette technologie ne présentent que peu d'intérêt pour un attaquant après avoir été présentées à un tiers. En tout état de cause, l'impact de ce risque doit aussi être pris en compte dans l'appréciation globale du service.

CRYPTOGRAPHIE A SEUIL

Cette technologie est mature et recommandée. Elle est très intéressante car elle permet d'accroitre la résilience des réseaux contre les attaques informatiques, et donc d'accroitre la cybersécurité des infrastructures. Elle élimine le risque d'attaque et de compromission d'un serveur unique contenant des clefs cryptographiques sensibles, en rendant nécessaire que plusieurs serveurs, possédant chacun une partie d'un secret (clef cryptographique), agissent de concert. Partant, une attaque informatique devient plus difficile à mener, car elle implique alors d'attaquer plusieurs serveurs et non plus un seul, ce qui améliore la résilience de l'infrastructure. Les risques induits par les points uniques de défaillance dans les architectures réseaux sont donc supprimés.

Cette technologie est aussi concernée par le risque de l'ordinateur quantique. Une nouvelle génération résistante à l'ordinateur quantique reste encore à inventer.

FIDO

Cette technologie est mature et recommandée pour les cas d'usage nécessitant uniquement une authentification du porteur. Un écosystème complet permettant l'usage de cette technologie est déjà déployé à grande échelle. En particulier, le standard FIDO2 sera bientôt nativement supporté dans la plupart des navigateurs Internet, cette évolution apportant notamment la capacité d'identification reposant sur des certificats cryptographiques liés à l'utilisateur. Cette technologie peut être utilisée (1) seule dans un système de gestion d'identité numérique pour l'identification et l'authentification d'un porteur souhaitant accéder à un service, ou (2) comme second facteur d'authentification renforçant un système d'identité numérique existant (par exemple basé sur un identifiant/mot de passe).

Cette technologie n'est en revanche pas adaptée en l'état actuel pour les cas d'usage nécessitant une identité et une authentification du porteur. En effet, elle ne prévoit ni ne permet la fourniture de données d'identité du porteur (nom, prénom…).

Par ailleurs, cette technologie n'apporte aucune réponse quant à la sécurité (1) du processus d'enrôlement du porteur quand il se voit délivrer une clef d'authentification FIDO correspondant à une identité ou des attributs qu'il

revendique - sans garantie, et (2) de la restauration des accès suite à une perte ou un vol du dispositif d'authentification. Tout système d'identité numérique s'appuyant sur cette technologie devra donc prévoir des procédures ou des solutions sécurisant ces étapes critiques de la technologie FIDO.

Cette technologie s'appuyant sur une cryptographie classique, est aussi concernée par le risque de l'ordinateur quantique.

CRYPTOGRAPHIE RESISTANTE A L'ORDINATEUR QUANTIQUE

Cette technologie n'est pas encore mature et ne le sera certainement pas avant cinq ans. Toutefois, la pression des technologies quantiques à laquelle elle doit déjà répondre ne peut pas être ignorée.

Aussi, l'introduction à terme de cette nouvelle génération de cryptographie doit être prise en compte dans tout programme d'identité numérique et ce dès le départ. Cela peut se faire de deux façons. Une première approche consiste à (1) lancer le système avec une cryptographie classique et (2) de prévoir une mise à jour du système à un horizon de 5 à 10 ans pour introduire cette nouvelle génération de cryptographie et éliminer la cryptographie de première génération. Cela implique de poser dès le premier déploiement une exigence de compatibilité ascendante du système, permettant de remplacer facilement la cryptographie classique par une cryptographie résistante à l'ordinateur quantique. Une seconde approche consiste à prévoir dès la mise en place du système une redondance, où l'utilisation de la cryptographie classique est doublée d'une cryptographie résistante à l'ordinateur quantique. Cette approche accroit par ailleurs la résilience globale du système car elle cumule la sécurité de chacune d'elles. La mise en défaut du système d'identité nécessiterait de pouvoir casser tout à la fois la cryptographie classique et la cryptographie post quantique, même si cette dernière n'est pas encore mature.

CHIFFREMENT BASE SUR L'IDENTITE ET SUR LES ATTRIBUTS (IBE, ABE)

Cette technologie est mature, et quelques solutions la mettant en œuvre ont émergé au cours des dernières années. Malheureusement, celles-ci n'ont pas percé, par manque d'intérêt ou de compréhension de cette technologie par le marché. Aussi un déploiement à moyen terme est envisageable, une fois que le marché aura été sensibilisé aux avantages notables de cette technologie.

La variante de cette technologie IBE, est, elle aussi, mature et utilisable. Quelques solutions commerciales existent pour le chiffrement de courriels.

Cette technologie est le futur du contrôle d'accès à des données sensibles – comme par exemple peuvent l'être les données d'identité. Alors qu'aujourd'hui le contrôle d'accès à des données est assuré par une autorité centrale qui héberge les données sensibles en (1) authentifiant les demandeurs et (2) vérifiant leurs

autorisations - créant par la même un point unique de défaillance, cette technologie permet d'éliminer cette faiblesse. En effet elle permet d'assurer un contrôle d'accès natif, reposant non pas sur une authentification auprès d'une autorité centrale, mais sur l'aptitude du demandeur à déchiffrer les données sensibles à l'aide de sa clef de déchiffrement reflétant ses autorisations.

Cette technologie est aussi concernée par le risque de l'ordinateur quantique, et une nouvelle génération résistante à l'ordinateur quantique reste encore à inventer. Néanmoins, au regard des bénéfices substantiels qu'elle apporte, **cette technologie est recommandée**, à condition toutefois de mettre en œuvre une gestion de risque permettant de limiter les conséquences de l'apparition de l'ordinateur quantique, et en particulier le risque de dévoilement des données à moyen-long terme.

Toutefois, cette technologie souffre de défauts importants. Tout d'abord une autorité centrale est nécessaire pour générer les clefs correspondant aux attributs (ABE) ou à l'identité du porteur (IBE). D'autre part, cette technologie n'offre pas de solution pleinement satisfaisante pour gérer la révocation d'un utilisateur. Son application est donc davantage cantonnée à des situations bien particulières, économiques mais plus approximatives en termes de fiabilité

ACCREDITATIONS ANONYMES (ABC)

Alors que la connaissance scientifique sur cette technologie est très avancée, ce n'est pas le cas des solutions et des applications utilisant cette technologie. Elles butent sur deux écueils majeurs. Tout d'abord il n'y a pas de standards permettant une mise en œuvre de telles solutions et applications de manière interopérable. Enfin de nombreux brevets couvrent cette technologie, bien que beaucoup d'entre eux arrivent à échéance. En cela, **cette technologie est en voie de maturité, et n'est donc recommandée qu'à moyen terme**.

Pourtant, la technologie ABC promet de remplacer l'authentification d'une entité auprès d'un tiers pour accéder à une ressource, par la démonstration par celle-ci de ses droits auprès du tiers. En cela, cette technologie permet de mettre en œuvre des mécanismes beaucoup plus respectueux des données personnelles et de l'anonymat, car étant beaucoup plus frugale en données.

CHIFFREMENT HOMOMORPHE

Cette technologie n'est pas totalement mature du point de vue scientifique car certains aspects restent encore à étudier. Néanmoins **elle est suffisamment mature pour permettre le développement de solutions basées sur cette technologie et leur utilisation à grande échelle**. Par ailleurs, ce domaine de recherche étant très actif, de nombreux progrès sont encore à attendre dans le futur, en particulier en termes de performance d'exécution.

De nombreuses librairies en « open source » existent, et des solutions basées sur cette technologie commencent ainsi à être proposées, en particulier par de jeunes pousses innovantes. Toutefois, l'absence de standard couvrant cette technologie reste un frein à son développement.

En particulier, cette technologie promet une révolution dans la manière de traiter des données sensibles - comme le sont par exemple des données d'identité ou des attributs relatifs aux personnes – en permettant à des tiers tout à la fois (1) de les traiter et de les analyser, et (2) de les leurs masquer de sorte à protéger l'anonymat de la personne à qui elles se rapportent. **En cela, cette technologie est donc recommandée.**

Enfin l'impact de l'ordinateur quantique sur cette technologie n'est pas encore bien connu. Alors que les modes basés sur la cryptographie classique (de type El Gamal) seront bien sûr cassés, ceux basés sur les réseaux euclidiens ne sont pas encore suffisamment connus et étudiés pour garantir qu'ils lui seront résistants.

ACN

Alliance pour la confiance numérique

A propos de l'ACN

L'Alliance pour la Confiance Numérique (ACN) représente les entreprises (leaders mondiaux, PME, et ETI) du secteur de la confiance numérique notamment celles de la cybersécurité, de l'identité numérique, des communications sécurisées, de la traçabilité / lutte anti-contrefaçon et de la safe city. La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur.

On dénombre environ 850 entreprises réalisant en France près de 9 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (plus de 12% de croissance chaque année depuis 2014).

Les membres de l'Alliance pour la Confiance Numérique (ACN), dont 65% de PME-ETI, représentent plus de 70% du chiffre d'affaires du secteur de la Confiance Numérique repartis sur l'ensemble de la chaine de valeur (fabricants de matériel, éditeurs de logiciels, intégrateurs, services, recherche, …).

L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication) et participe activement aux travaux du CSF (Comité Stratégique de Filière) des Industries de Sécurité.

Par ailleurs, l'ACN est également membre fondateur de l'ECSO (European CyberSecurity Organisation).

www.confiance-numerique.fr