

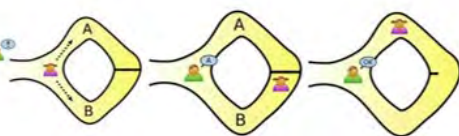
Prouver la connaissance d'un secret sans le divulguer

Les protocoles de preuves
à divulgation nulle de connaissances



Lundi 24 novembre
18h00 - 20h00

Par webinaire Zoom



Protocoles zero-knowledge Prouver la connaissance d'un secret sans le divulguer



Jean-Jacques Quisquater
Cryptologue Belge
Professeur à l'université
catholique de Louvain

Organisateurs



Pr Ahmed Mehaoua
Université Paris Cité



Batrice Laurent et Gérard Peliks
avec Jean-Jacques Quisquater

Comment prouver qu'on connaît le contenu d'un message sans le divulguer ?



Bob : Bonjour Alice

Alice : Bonjour Bob

Bob : Alice, j'ai un message important et je veux te prouver que je connais son contenu

Alice : Eh bien envoie le-moi ton message, Bob, comme cela, étant deux à connaître son contenu, tu m'auras prouvé que tu détiens bien ce message



Bob : Non, il n'en est pas question Alice ! le contenu de ce message est très confidentiel, je veux seulement te prouver que je l'ai, mais sans que tu saches ce qu'il contient.

Alice : Je ne vois pas comment ce serait possible, même pour un cryptologue comme toi, Bob, tu n'es pas un magicien que je sache ?

Bob : Mais bien sûr que c'est possible Alice, en utilisant un protocole de **preuves à divulgation nulle de connaissance : un ZKP** : un **Z**ero-**K**nowledge **P**roof.

Alice : C'est quoi un ZKP ??? Te connaissant, Bob, c'est encore une question de cryptologie et de mathématiques très poussées ? Explique-moi comment tu ferais, mais simplement et d'une manière telle que je puisse le comprendre.

Gérard : Bon quittons ces deux personnages, Alice et Bob, bien connus des cryptologues. Je reprends la main. **La cryptologie, est-ce vraiment de la magie ?** En fait, un cryptologue se comporte bien comme un magicien. On pense que les tours de passe-passe d'un bon magicien reposent sur de la magie mais en fait, le magicien est seulement très adroit. Il ne fait qu'utiliser un trucage bien réel mais que personne ne remarquera. Le cryptologue est comme le magicien, son truc c'est une méthode et un algorithme.

Jean-Jacques Quisquater, professeur au mérite de l'université catholique de Louvain (un cryptologue Belge que nous sommes fiers de compter comme éminent professeur à l'ARCSI) nous expliquera de manière compréhensible ce truc au « Lundi de la Cybersécurité » du mois de novembre, le **lundi 24 novembre, par webinaire de 18 h 00 à 20 h 00**.

Les preuves à divulgation nulle de connaissance (c'est ça le truc) sont très utiles en cryptologie, par exemple pour s'authentifier de manière sûre et sans recourir aux mots de passe, ou pour permettre des transactions anonymes dans des blockchains.

Un Lundi de la Cybersécurité à ne pas rater durant lequel le professeur Jean-Jacques Quisquater nous expliquera cette facette de la cryptologie, en excellent pédagogue qui sait se faire comprendre par tous les niveaux de publics, et dont on retire une connaissance qui peut être très utile du sujet traité.

Jean-Jacques a déjà animé plusieurs de nos « Lundi de la Cybersécurité », comme celui de novembre 2023 sur « la cryptologie post quantique » ou comme celui de novembre 2022 sur « les attaques par canaux cachés ». Décidemment, avec une telle personnalité, nos « Lundi de la Cybersécurité de novembre » connaissent toujours un très grand succès.

Je donne la plume au professeur Jean-Jacques QUISQUATER



Quand on a un secret il vaut mieux le garder seulement pour soi. Ce que permet par exemple l'utilisation des systèmes dits à clés publiques : si je signe un fichier par le RSA avec ma clé secrète cela *prouve* que je connais la factorisation du module entier utilisé sans l'exposer : ce n'est pas tout-à-fait une preuve en fait avec plein de fuites possibles autres que matérielles. Les protocoles zero-knowledge (à divulgation ou apport nul de connaissance) vise mieux et plus haut pour obtenir une preuve de connaissance sans rien révéler d'autres. C'est aussi ce qu'apporte souvent un tour de magie : j'ai un pouvoir secret (souvent de manipulation) qui permet de le montrer sans décrire le "truc". Oui, la cryptographie ressemble beaucoup à la magie : nous le verrons par des exemples pédagogiques.

Ces protocoles ont une longue histoire : elle commence en 1985 avec un article fondateur de Goldwasser, Micali et Rackoff. En fait, Fischer, Micali et Rackoff présentent à Eurocrypt 84, à Paris, une première version qui disparaît des proceedings pour n'être publiée qu'en 1996 (!). Puis Fiat et Shamir publient à CRYPTO 1986 une version pratique qui sera utilisée par les décodeurs de TV à péage. En fait, deux mois avant, Shamir présentera ce protocole à une réunion du CIRM à Marseille : Louis Guillou et moi-même y étions présents. Nous percevons

très vite l'intérêt pour les cartes à puce et nous constatons que cela demande beaucoup de ressources. Il en viendra alors le protocole GQ (1988) demandant le minimum d'échanges mais encore gourmand en calculs. Puis ce sera GQ2 (2001) bien mieux économe mais plus compliqué. Philips France me demanda de convaincre leur direction d'utiliser GQ : et ce fut l'histoire d'Ali-Baba. Tout cela ne fut pas facile car nous avions un brevet GQ qui a d'abord été stoppé en France, vu son caractère cryptographique mais finalement assez vite libéré mais il en fut tout autre aux USA car la NSA ne voulait pas que l'on utilise GQ, qui est finalement une version dérivée du RSA, ce qui aurait permis, par détournement, du chiffrement alors honni (voir PGP).

Finalement, sauf récemment, ces protocoles ont été peu utilisés malgré leurs avantages (merci à Gemplus et David Naccache d'avoir réalisé des cartes à puce GQ2). Maintenant, ces protocoles sont en grande vogue pour améliorer les procédures de login, l'usage des cryptomonnaies (zcash notamment) et des blockchains. Des exemples, plus théoriques, sont la possibilité de prouver que l'on connaît un résultat mathématique (une démonstration par exemple) sans l'exposer. Etc. La suite lors de la présentation.

Qui est Jean-Jacques QUISQUATER ?



Jean-Jacques Quisquater est professeur émérite (au mérite) de cryptologie et de sécurité multimédia au département d'électricité (ICTEAM), à l'École polytechnique de Louvain (EPL), en Belgique. Il est co-inventeur du schéma d'identification zero-knowledge Guillou-Quisquater, utilisé dans des cartes à puce et par Novell. Il est membre à vie de l'IEEE, académicien titulaire émérite à l'Académie royale de Belgique, chercheur associé au MIT entre 2004 et 2022 et membre d'honneur de l'ARCSI. De plus il est IACR fellow, a reçu le prix d'excellence en mathématiques de la conférence RSA.



Il a été chercheur chez Philips durant plus de 20 ans (recherches sur la théorie des FPGA, le dessin automatique de circuits, puis la cryptologie depuis 1979 et la théorie des graphes), puis professeur invité à Lille, Namur, en plus de l'UCLouvain. Il a eu la première chaire Fermat à Toulouse et une chaire Francqui en Belgique. Un prix Montefiore lui a été attribué. Il a été invité durant 6 mois comme directeur de recherches du CNRS, a donné cours de cryptographie à ENS-Ulm durant 12 ans et donne encore cours à ESIEA.

Il a 20 brevets et près de 700 publications d'après Google Scholar (ceci inclut les articles dans les journaux d'actualités). Il est cité par Satoshi Nakamoto dans le papier fondateur de bitcoin (référence 2 de 8).

Demande d'inscription au lundi 24 novembre, par visio-conférence à partir de 18 h 00.



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien pour entrer dans la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à **Béatrice Laurent** co-organisatrice de nos évènements :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux

intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@noos.fr).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 24 novembre, dès 18 h 00 ou mieux, un peu avant**. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00** pour des conversations informelles entre intervenants et participants. Ce sont toujours d'agréables échanges qui se font avant 18 h 00.

Quelques minutes avec une association : le CCB - Centre pour la Cybersécurité Belgique

Suivant la tradition de nos « *Lundi de la cybersécurité* », entre l'exposé des intervenants et la session questions / réponses, qui commence autour de 19 h 30, nous donnons pour une quinzaine de minutes la parole à une organisation ou à une personne qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Cette séquence des **quelques minutes avec une association** sera animée par **Phédra CLOUNER**

Phédra CLOUNER est Directrice Générale Adjointe du Centre pour la Cybersécurité Belgique (CCB), l'autorité nationale pour la cybersécurité qui supervise la mise en œuvre de la stratégie nationale de cybersécurité et œuvre à faire de la Belgique l'un des pays les moins cyber-vulnérables en Europe. Elle a précédemment exercé les fonctions de CISO au ministère belge de la Justice et a occupé des responsabilités dans la gestion de l'information, le business intelligence et la gestion de contenu web.



En plus de son rôle au sein du CCB, elle occupe des postes de direction dans des initiatives nationales et européennes en cybersécurité, notamment en tant que Vice-Présidente de la Belgian Cybersecurity Coalition et membre fondatrice de Women4Cyber Belgium.

Le CCB est pour la Belgique l'équivalent de l'ANSSI pour la France.

La Belgique a été le premier état de l'Union européenne à avoir transposé la directive NIS2 dans ses lois. Voyez ce que Phédra Clouner en dit : <https://www.solutions-magazine.com/nis2-un-an-plus-tard/>. De plus dans le domaine de la cryptographie, l'algorithme standard dans le chiffrement symétrique, l'AES – Advanced Encryption Standard - est l'œuvre de deux chercheurs Belges, Joan Daemen et Vincent Rijmen.

Oui, la Belgique, pour la cybersécurité, est une source d'inspiration, et nous sommes fiers que Phédra s'exprime à la suite de Jean-Jacques Quisquater et les deux répondront ensuite à nos questions à partir de 19 h 30. Quelle soirée sera ce lundi de novembre !!!

Le coin des « *Lundi de la cybersécurité* » précédents.

Vous trouverez, sur le web de l'ARCSI en https://www.arcsi.fr/evt_passes.php tous les détails, slides, parfois aussi les enregistrements et des comptes rendus.

Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?

Prompt posé à ChatGPT (jusqu'à la lettre précédente, c'était à Gemini, là nous changeons):

Quelles sont les applications du protocole de preuves à divulgation nulle de connaissances ?

Réponse de ChatGPT :

Les **preuves à divulgation nulle de connaissances** (*Zero-Knowledge Proofs*, ZKP) sont un outil cryptographique puissant permettant à une partie (le **prouveur**) de convaincre une autre (le **vérificateur**) qu'une affirmation est vraie **sans révéler d'information autre que la validité de l'affirmation**.

Elles trouvent des applications dans de nombreux domaines :

1. Authentification sécurisée

- Permet de prouver son identité **sans transmettre de mot de passe** ni de clé secrète.
- Exemples :
 - o Connexions à des systèmes informatiques sans risque d'interception des identifiants.
 - o Protocoles d'accès dans l'IoT ou les cartes à puce.

2. Cryptomonnaies et Blockchain

- **Zcash** utilise des ZKP (zk-SNARKs) pour offrir des transactions privées et vérifiables.
- **Ethereum** expérimente des ZKP pour la scalabilité (zk-rollups).
- Applications :
 - o Anonymisation des transactions (confidentialité).
 - o Preuve qu'une transaction est valide sans révéler les détails (montant, adresses).
 - o Amélioration de la performance des blockchains (agrégation de preuves).

3. Systèmes financiers et e-voting

- **Paiements confidentiels** : prouver qu'un transfert respecte les règles (ex. solde suffisant) sans divulguer les montants.
- **Vote électronique** :
 - o Un électeur peut prouver qu'il a voté correctement sans révéler pour qui.
 - o Garantit l'anonymat tout en permettant de vérifier l'intégrité du scrutin.

4. Protection de la vie privée et conformité

- **KYC / AML (Know Your Customer / Anti-Money Laundering)** :
 - o Une personne peut prouver qu'elle est majeure ou réside dans un pays autorisé **sans révéler son identité complète**.
- **Conformité réglementaire** : prouver qu'une institution respecte certaines règles (capital minimum, réserves bancaires, etc.) sans divulguer toutes ses données financières.

5. Cloud computing et vérification déléguée

- Permet à un client de vérifier qu'un calcul effectué par un serveur est correct **sans avoir à le refaire**.
- Applications dans :
 - o Vérification de données stockées dans le cloud.
 - o Sécurité des contrats intelligents et calcul multipartite.

6. Applications industrielles et IoT

- Authentification des objets connectés sans échange de secrets sensibles.
- Vérification sécurisée de certificats, de licences logicielles ou de droits d'accès.

Les ZKP sont essentiels dans tout contexte où **confidentialité** + **vérifiabilité** doivent coexister.

On les retrouve particulièrement dans la **finance numérique**, la **protection de la vie privée**, l'**authentification**, et de plus en plus dans la **blockchain et le cloud computing**.

Nous écouterons **Jean-Jacques QUISQUATER** nous dire ce qu'il en pense.

Inscrivez-vous (mail à beatricelaurent.cde@gmail.com) ou cliquez ici :

JE M'INSCRIS

Gérard

