ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte rendu du Lundi de la cybersécurité du 13 avril 2026

Protocole zero-knowledge : prouver la connaissance d'un secret sans le divulguer

Présenté par Jean-Jacques QUISQUATER

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks
Rédigé par Rayan Al Mohaize, étudiant en Master 2 Cybersécurité

Table des matières

I Introduction

L'événement « Lundi de la Cybersécurité » est une série mensuelle de conférences en ligne organisée de manière indépendante par Gérard Peliks et Béatrice Laurent. Elle a pour vocation d'explorer chaque mois une thématique différente liée aux enjeux contemporains de la sécurité numérique et de la société.

1 Le thème de la cryptographie et du zero-knowledge

Le Lundi de la cybersécurité du 13 avril 2026 portait sur les protocoles zero-knowledge et la manière de prouver la connaissance d'un secret sans le divulguer. Lors de ce webinaire, Jean-Jacques Quisquater nous a présenté un pilier de la cryptographie moderne : le zero-knowledge, ainsi que son application concrète à travers le protocole GQ, dont il est le co-inventeur. Nous avons également découvert les domaines dans lesquels les travaux de Jean-Jacques Quisquater sont utilisés et à quel point ils ont influencé le monde moderne, notamment dans le domaine des cryptomonnaies.

2 Les intervenants

Pour animer ce Lundi de la cybersécurité, Jean-Jacques QUISQUATER nous a fait l'honneur de nous présenter le protocole zero-knowledge et la notion de secret en cryptologie. Jean-Jacques QUISQUATER est professeur émérite de cryptologie et de sécurité multimédia à l'École polytechnique de Louvain en Belgique, ainsi que co-inventeur du schéma d'identification zero-knowledge Guillou-Quisquater, utilisé notamment dans des cartes à puce.

Par la suite, Phédra CLOUNER a animé le quart d'heure des associations pour présenter le CCB (Centre pour la Cybersécurité de Belgique) dont elle en est la directrice générale adjointe.

II Protocole zero-knowledge : prouver la connaissance d'un secret sans le divulguer (par Jean-Jacques QUISQUATER)

D'après le Larousse, une preuve est un élément matériel, un témoignage ou un raisonnement servant à établir de manière certaine la vérité ou la réalité d'un fait, d'un acte ou d'un sentiment. Elle permet de démontrer, de vérifier ou d'attester une affirmation. Cependant, en prenant la définition rigoureuse, notamment dans le cadre du zero-knowledge, cette définition du Larousse laisse supposer qu'il reste toujours un élément de probabilité non nul, que l'affirmation à prouver est fausse, et que l'on peut faire tendre cette probabilité vers 0. Ainsi le terme français correct pour exprimer cette définition, c'est le terme de vraisemblance. C'est avec ce petit détail que Jean-Jacques QUISQUATER commence sa présentation.

Pour encore mieux comprendre la notion de preuve et de vraisemblance, nous sommes revenus sur un cours de mathématiques donné à UC Louvain en 2012 sur le contrôle d'accès basique avec identifiant et mot de passe (login), impliquant un prouveur et un vérifieur et les différents problèmes qui y sont liés :

— Du côté du prouveur : vol de mot de passe, usurpation d'identité.
— Du côté du vérifieur : faux terminal, espionnage, plusieurs terminaux peuvent vérifier.

Pour remédier à cela, plusieurs solutions sont proposées par Jean-Jacques QUISQUATER : utiliser des mots de passe uniques (OTP) ou bien ne pas utiliser de mot de passe du tout. Dans le cas où l'on n'utilise pas de mot de passe du tout, l'idée serait de prouver que l'on possède le mot de passe sans le donner et de fournir une nouvelle preuve à chaque interaction. Cela impliquerait donc l'intervention du vérifieur qui va questionner le prouveur toujours de manière différente à chaque interaction pour obtenir la preuve de la détention du mot de passe. Ainsi chaque échange est unique entre le prouveur et le vérifieur. C'est exactement comme cela que fonctionne le zero-knowledge.

Jean-Jacques QUISQUATER nous présente les principales propriétés du zero-knowledge :

— Complétude : Un prouveur qui connaît l'information secrète peut le prouver avec une probabilité de 1.
— Solidité : La probabilité qu'un prouveur ne connaissant pas l'information secrète puisse réussir à tromper le vérificateur peut être rendue arbitrairement petite.

2 La genèse du zero-knowledge et du protocole GUILLOU- QUISQUATER (GQ)

L'étude marquant le point de départ du zero-knowledge a été l'article de Shafi GOLDWASSER, Silvio MICALI et Charles RACKOFF intitulé *The Knowledge Complexity of Interactive Proof Systems* et publié en 1985.

Un an plus tard, en 1986, un autre article fondateur de la notion de zero-knowledge apparaît, intitulé *How to prove yourself : practical solutions to identification and signature problem* par Amos FIAT et Adi SHAMIR. Ces derniers ont repris l'étude de GOLDWASSER, MICALI et RACKOFF et l'ont rendue pratique en créant le protocole FIAT SHAMIR permettant essentiellement de prouver son identité ou la validité d'une affirmation sans révéler de secret.

À la suite de la publication de l'article de FIAT SHAMIR et de la mise en place de leur protocole, Jean-Jacques QUISQUATER, accompagné de Claude GOUTIER, Yvo DESMEDT et Gilles BRASSARD, publie l'article *Secure Implementation of Identification Systems* en 1987, proposant des solutions pour sécuriser le protocole FIAT SHAMIR.

Enfin, à l'issue de toutes ces études ayant posé les bases du zero-knowledge, Jean-Jacques QUISQUATER et Louis GUILLOU ont réussi à généraliser le protocole de FIAT SHAMIR en prouvant que l'on peut connaître un nombre, sans le donner, et le résultat, l'output, s'approche d'un nombre aléatoire, mais pas totalement : basé sur l'exponentielle discrète et le RSA. Cela donne donc naissance au protocole GQ (GUILLOU QUISQUATER) formalisé par ces derniers dans l'article *A "Paradoxical" Indentity-Based Signature Scheme Resulting from Zero-Knowledge.* publié en 1988.

2 L'application concrète du zero-knowledge et du protocole GQ

En 1996, Jean-Jacques QUISQUATER crée une puce pour carte à puce appelée SCALPS (Smart CArd for Limited Payment Systems), une puce zero-knowledge pour cryptomonnaies utilisant le protocole GQ. En effet, les preuves zero-knowledge que Jean-Jacques QUISQUATER a contribué à rendre pratiques (via GQ, SCALPS, etc.) sont aujourd'hui au cœur de certaines cryptomonnaies. Ces protocoles sont désormais en grande vogue pour améliorer les procédures de connexion, l'utilisation des cryptomonnaies et des blockchains. Les zk-SNARKs et zk-STARKs qui alimentent l'Ethereum et les transactions privées de la cryptomonnaie Zcash descendent directement de cette lignée théorique ("zk" pour zero-knowledge). Ce qui montre encore plus l'implication du protocole GQ dans les cryptomonnaies, c'est le fait que Quisquater est directement cité par le mystérieux Satoshi Nakamoto, créateur du Bitcoin, dans son célèbre livre blanc *Bitcoin : A Peer-to-Peer Electronic Cash System*

Par ailleurs, le zero-knowledge est utilisé en TV à péage pour authentifier les cartes des abonnés vis-à-vis du décodeur. La carte joue le rôle du prouveur et le décodeur joue le rôle du vérifieur.

Enfin, le protocole GQ a été beaucoup piraté en Afrique du Sud et particulièrement au Japon, où il n'a toujours pas été approuvé. Jean-Jacques QUISQUATER précise que le protocole ne sera jamais approuvé dans ces zones-là.

III Présentation du Centre pour la Cybersécurité de Belgique (Par Phédra CLOUNER)

Comme toujours, la seconde partie de ce Lundi de la cybersécurité est dédiée à un représentant d'une association pour lui donner l'opportunité de représenter ses objectifs et ses valeurs. Phédra CLOUNER, directrice générale adjointe du CCB, nous a donc fait l'honneur d'animer ce quart d'heure des associations.

1 Présentation du CCB

Le CCB, correspondant à l'équivalent de l'ANSSI, est un organisme relevant du Premier ministre ayant plusieurs rôles et missions :

- Intervenir en cas d'incident de sécurité (CSIRT/CERT)
- Coordonner la mise en œuvre de la stratégie nationale de cybersécurité
- Coordonner la mise en œuvre de la directive NIS2
- Centre national de coordination : chargé de centraliser les possibilités de financement européennes et nationales destinées à soutenir les investissements dans des projets de cybersécurité depuis 2021
- Autorité nationale de certification en matière de cybersécurité (NCCA) dans le cadre des systèmes de certification européens depuis 2022.

Le principal objectif de CCB est de faire de la Belgique l'un des pays les moins vulnérables dans le domaine cybernétique. Et pour cela, l'organisme mobilise des professionnels de la cybersécurité hautement technique (analystes, hackers éthiques, chercheurs, etc.) et d'autres domaines en tout genre (avocats, chefs de projet, chargés des relations internationales, spécialistes en communication, etc.). Ainsi, le CCB joue un rôle de coordination à la fois au niveau stratégique et au niveau opérationnel.

2 Une protection active contre les cyberattaques

Voici comment s'articule l'approche proactive, adaptée, automatisée et participative de la cybersécurité adoptée par le CBB :

- Proactif : Plutôt que de simplement réagir aux attaques, une recherche proactive des menaces et vulnérabilités potentielles pour renforcer la préparation et prévenir les violations de cybersécurité.
- Adaptée : Parce qu'il n'existe pas de solution universelle, des solutions personnalisées doivent prendre en compte les besoins différents des parties prenantes.
- Automatisée : Dans un paysage de cybersécurité en évolution rapide, la vitesse est essentielle et des solutions automatisées sont nécessaires pour protéger les systèmes contre des attaques de plus en plus automatisées.
- Participatif : Une implication active de tous les acteurs, des individus aux petites et grandes organisations, dans l'identification et la correction des vulnérabilités.

Pour impliquer les utilisateurs dans la cybersécurité en Belgique, le CCB a mis en place une plateforme à partir de laquelle toute personne recevant un message suspect pouvant être du phishing peut émettre une alerte et transmettre ces mails suspects au CCB. En 2017, seulement quelques centaines de mails ont été envoyés, et en 2026 près de 40 000 mails suspects sont envoyés par jour. Grâce à cela, des domaines malicieux sont identifiés et un pop-up s'affiche quand on accède à ces domaines. En 2025, ce pop-up est apparu près de 180 millions de fois en Belgique !

Le CCB a la possibilité de scanner l'intégralité de l'Internet belge pour identifier les menaces et prévenir les organisations vulnérables ou déjà infectées ou pour envoyer des alertes à des utilisateurs identifiés comme vulnérables : c'est le spear warning.

De plus, le CCB a mis en place une extension appelée Sefonweb Browser Extension pouvant être intégrée aux différents moteurs de recherche pour indiquer les sites à risques. Cela permet de donner un degré de confiance aux internautes via trois couleurs : vert pour les sites sécurisés, orange pour les sites à risque modéré, rouge pour les sites à risque élevé.