



*Le vendredi 25 septembre 2020, à 12 h*

**M. Jean-Jacques QUISQUATER, Professeur émérite à l'École Polytechnique de l'Université Catholique de Louvain**

*traitera du sujet suivant :*

## **La cryptographie : comment concilier sobriété numérique et sécurité ?**



*Jean-Jacques QUISQUATER est un cryptographe belge de renommée mondiale, notamment en tant que co-inventeur du schéma d'identification Guillou-Quisquater, protocole largement utilisé dans le monde. Titulaire d'un Master d'ingénieur en mathématiques appliquées de l'École Polytechnique de l'Université Catholique de Louvain, il a par la suite obtenu un Doctorat d'État en science informatique au Laboratoire de Recherche en Informatique de l'Université de Paris-Saclay à Orsay.*

*Après avoir travaillé 20 ans au laboratoire de recherches de Philips, où il a dirigé un groupe de recherche qui a mené à l'application de la cryptographie dans les cartes à puce, il est entré au département d'électricité de l'École Polytechnique de l'UCL, où il est devenu professeur de cryptographie et de sécurité multimédia. Il est conseiller scientifique de l'« UCL Crypto Group », qu'il a dirigé avant d'être admis à l'éméritat. Il a enseigné et/ou mené divers travaux de recherche dans diverses universités, notamment au MIT, dont il est toujours chercheur affilié.*

*Il détient 17 brevets dans le domaine de la carte à puce et de la sécurité informatique et a publié quelque 200 articles dans des revues ou pour des conférences internationales. Il est membre de l'Académie Royale de Belgique, membre correspondant de l'Académie des Sciences de Toulouse, membre de l'IEEE ( Institute of Electrical and Electronics Engineers ) et d'autres associations internationales. Il a été fait docteur honoris causa des Universités de Limoges et de Toulouse, et a en outre reçu de nombreuses distinctions.*

*A titre personnel, il collabore à des recherches concernant la compréhension des quipus incas.*

Notre orateur expliquera d'abord ce qu'est la cryptographie et quels en sont ses différents usages. Il s'agit d'une technique ( dont l'origine remonte à l'Antiquité ) destinée à assurer la confidentialité, l'authenticité et/ou l'intégrité des messages, essentiellement aujourd'hui ceux transmis par le numérique. Pour cela, elle utilise souvent ce que l'on appelle une 'clef'. La prolifération actuelle des 'objets' connectés ( comptes bancaires, commerce électronique, WiFi, téléphones mobiles, ... ), tout comme celle des piratages informatiques, justifie l'importance de la cyber-sécurité.

Mais le numérique a également un impact environnemental important ( près de 4% des émissions de gaz à effet de serre ), ce qui impose de rechercher une certaine sobriété numérique. Notre orateur montrera qu'il y a une contradiction entre les objectifs de cyber-sécurité et ceux de sobriété numérique, car beaucoup d'algorithmes cryptographiques sont fort gourmands. De plus, les ordinateurs quantiques peuvent arriver assez rapidement sur le marché, et il est donc nécessaire de développer de nouveaux algorithmes adéquats, qui seront encore plus gourmands.

Enfin, notre orateur terminera son exposé en soulignant qu'il y a aussi, dans le domaine de l'informatique,

une certaine contradiction entre obsolescence matérielle et logicielle d'une part, et meilleure cyber-sécurité d'autre part.

**Lieu** : Château Sainte-Anne, rue du Vieux Moulin, 103 à 1160 Bruxelles, où nous vous attendons à **12 h** pour l'apéritif, suivi du déjeuner et de la conférence.

**Participation** ( apéritif, repas, vins et café compris ) : **50 €/pers.** pour les membres **SEII** ou **CSA** en règle de cotisation et leur conjoint(e) – **65 €/pers.** pour les non-membres, à verser au compte **BE63 3101 3976 9208** ( BBRUBEBB ) de la SEII, en précisant bien le **nom du participant** et la **référence de l'événement**.

### **Dispositions spéciales dans le cadre de l'épidémie de Covid-19**

**Il est obligatoire de porter un masque ( sauf à table pour boire et manger ) : tout participant ne portant pas de masque sera refusé**

**Vous êtes priés de vous asseoir à table dès votre arrivée, où l'apéritif vous sera servi**

**Le nombre de convives par table étant limité, le nombre total de convives sera également limité : si ce nombre total est atteint, c'est sur base des payements reçus que nous nous baserons**

Pour vous inscrire, **pour le 22 septembre au plus tard**, un formulaire est accessible via notre site web : [www.seii.org](http://www.seii.org)

Il est également possible de **s'inscrire par e-mail** à [info@seii.org](mailto:info@seii.org) en précisant clairement vos nom, prénom, n° de téléphone, les nom(s) et prénom(s) d'(un) éventuel(s) invité(s), l'événement auquel vous vous inscrivez, si vous êtes ou non membre de la SEII ou du CSA, et le montant que vous vous engagez à régler.

**Attention** : votre réservation à ce déjeuner conférence ne sera assurée que si le montant dû est crédité au compte bancaire de la SEII **au plus tard 48 heures avant l'événement – 72 h si le paiement sert d'unique moyen d'inscription** – ( car nous ne pouvons réserver le nombre de repas qu'en fonction de l'argent reçu ).  
*Merci de votre compréhension.*

**Pour une désinscription au moins 48 heures avant la conférence, aucun frais ne vous sera réclamé.**

---

**SEII ( Société Européenne des Ingénieurs et des Industriels )**, asbl – Rue d'Egmontstraat, 11 - 1000 Brussels – TVA : BE 0471 474 339  
Tél : +32 (0)472 707 767 – URL : [www.seii.org](http://www.seii.org) – E-mail : [info@seii.org](mailto:info@seii.org) – IBAN : BE63 3101 3976 9208 – BIC : BBRUBEBB

---

*Diverses données « non-sensibles » vous concernant sont enregistrées dans un fichier propre à la SEII, afin de pouvoir communiquer avec vous : vous tenir informé de nos activités et, si vous êtes membre de la SEII, vous envoyer les appels à cotisation. En conformité avec le RGPD – Règlement Général sur la Protection des Données – entré en vigueur en Europe le 25 mai 2018, nous pouvons à votre demande vous faire connaître les données enregistrées à votre nom, les corriger si nécessaire, ou les effacer de nos listes de mailing si elles ne sont pas requises dans le cadre d'un accord formel ou tacite.*

---