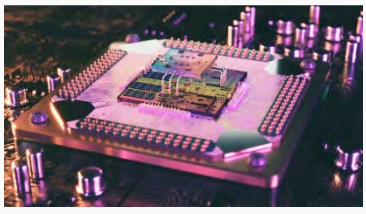
Lettre des "Lundi de la cybersécurité" n° 63

Quand tout devient quantique
Ordinateurs, communications, algorithmes résistants

Quand tout devient quantique :
Ordinateurs, communications, algorithmes résistants

Attention à ne pas confondre les technologies quantiques appliquées à la cryptologie, les calculateurs quantiques et la cryptologie dite « post quantique ».



Les calculateurs quantiques, quand ils auront suffisamment de qubits actifs seront une menace pour les algorithmes de chiffrement asymétriques actuels, dits chiffrement à clés publiques, et imposeront des clés plus longues pour le chiffrement symétrique.

La cryptologie post-quantique sera alors une évolution nécessaire des algorithmes de chiffrement, pour le chiffrement asymétrique, comme le RSA. Cette cryptologie est dite post quantique parce qu'elle viendra après que les calculateurs quantiques auront

atteints leur maturité et leurs propriétés seront exploitées par les nouveaux chiffrements.

Les technologies quantiques, qui sont déjà utilisées depuis des années, sont basées sur les propriétés de la physique quantique essentiellement pour deux fonctions :

1. La **distribution quantique de clés** (QKD : quantum key distribution) pour le chiffrement symétrique en garantissant une impossible compromission entre l'entité qui chiffre et celle qui déchiffre. Ce protocole est basé sur la propriété d'intrication quantique.
2. **La génération quantique de nombres réellement aléatoires** pour constituer les clés secrètes utilisées dans le chiffrement symétrique, comme l'AES. Les ordinateurs ne peuvent générer que des nombres pseudo-aléatoires, ce qui est une faiblesse pour le chiffrement classique, car si on peut déterminer une clé produite, la confidentialité est bien sûr remise en question. Une clé fiable a besoin d'être constituée de vrais aléas et la physique quantique par les propriétés d'intrication et de décorrélation produit ce genre d'aléas purs.

La cryptologie post quantique résistera aux tentatives de décryptement faits au moyen de calculateurs quantiques. Mixer dès à présent le chiffrement classique et ce qui existe pour le chiffrement post quantique est une solution conseillée par l'ANSSI.

Mais je ne suis qu'un béotien en la matière, par contre nous avons trouvé un des meilleurs experts du sujet, le professeur Jean-Jacques Quisquater, je m'efface devant lui.

Je donne la plume à Jean-Jacques Quisquater

Nous parlerons de ces trois domaines en montrant ce qu'ils ont de commun et, surtout, de différent.

Nous ferons le point sur les ordinateurs quantiques pour comprendre ce qu'ils peuvent apporter à la cryptanalyse des algorithmes cryptographiques classiques (RSA, ECC, DH, AES, SHA, ...) : nous verrons ensuite ce que cela implique dans le futur comme nouveaux algorithmes avec tout ce que cela comporte : implémentations, tests, flexibilité, normes, contributions de la France et de l'Europe ...

Et, aussi, moins connu, les implications géopolitiques dans le contexte de luttes économiques entre USA et Chine (l'Europe compte ici à peine les points).

L'exposé sera très accessible. Les communications seront aussi abordées pour bien préciser chacun des trois domaines.

Je reprends la plume

Qui est le Professeur Jean-Jacques Quisquater ?

Jean-Jacques Quisquater est un cryptologue belge, professeur à l'université catholique de Louvain, et membre de l'ARCSI. Docteur d'État en science informatique obtenu au Laboratoire de recherche en informatique de l'université d'Orsay, il est membre de l'IEEE.

Il est co-inventeur du schéma d'identification Guillou-Quisquater utilisé dans les cartes à puce. Il est membre de l'académie royale de Belgique, chercheur associé au MIT et ancien enseignant en cryptographie à l'ENS-Ulm.

Demande d'inscription pour le Lundi de la cybersécurité du mois de novembre

Lundi 20 novembre, à partir de 18 h 00, en ligne par visio-conférence Zoom.

Cet évènement se fera **en distanciel par Zoom**,

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 personnel vers la visioconférence.

Les demandes d'inscriptions sont à adresser à :

beatricelaurent.CDE@gmail.com

Dans votre message d'inscription, nous apprécierions que vous écriviez quelques mots sur vous et sur l'intérêt que vous accordez au sujet traité. Evitez le style télégraphique, nous sommes toujours heureux de vous lire et de connaître votre intérêt pour nos événements.

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

Si vous souhaitez ne plus recevoir les lettres des « Lundi de la cybersécurité »

mensuels, une simple demande par mail suffit. Si vous voulez être ajoutés à la liste de distribution, demandez-le nous.
Et bien entendu, si vous vous inscrivez pour assister à notre évènement, soyez connectés le lundi 20 novembre.

Quelques minutes avec …

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19 h 15, nous donnons pour une dizaine de minutes la parole à une organisation, qui opère dans l 'écosystème du numérique et dans la sécurité de l'information.

Le nom de l'invité surprise et de son organisation vous seront donnés bientôt.

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez tous les détails, slides, parfois aussi les enregistrements sur le web de l'ARCSI, en **https://www.arcsi.fr/.** pour les plus récents. Les événements plus anciens sont en **https://www.arcsi.fr/evt_passes.php.**
Les enregistrements des organisations qui sont intervenues durant les « quelques minutes » se trouvent en première page du site de l'ARCSI, là où sont les logos de ces organisations. Cliquez sur un logo, vous obtenez l'enregistrement s'il a été fait.

Nous remercions Francis Bruckmann, webmestre et membre du Conseil d'Administration de l'ARCSI pour son travail qui constitue la mémoire de nos événements.

Les 15èmes rencontres de l'ARCSI

Les 15èmes rencontres de l'**A**ssociation des **R**éservistes du **C**hiffre et de la **S**écurité de l'**I**nformation se tiendront en présentiel uniquement, le **mardi 5 décembre à la Bibliothèque Nationale de France** –avenue de France - 75013 Paris. Voici le thème de cette grande manifestation annuelle de l'ARCSI : « ***L'emballement des progrès technologiques en matière de numérique ne met-il pas en péril la sécurité de l'information ?*** ».

Plusieurs intervenants seront ceux que nous avons eu le plaisir d'écouter dans nos Lundi de la Cybersécurité récents. Le matin sera consacré aux problèmes induits par l'accumulation des technologies du numérique, l'après-midi à leurs solutions.

Les inscriptions à cet évènement gratuit se feront sur www.arcsi.fr.

Nous communiquerons bientôt sur cet évènement. Restez à l'écoute.

Le coin coin de l'IA générative

Question posée à Chat GPT, et sans livrer, bien sûr, de données confidentielles qui pourraient être exploitées :

Le calculateur quantique est-il une menace pour la cryptographie d'aujourd'hui ?

Réponse reçue :

Le calculateur quantique est souvent considéré comme une menace potentielle pour la cryptographie d'aujourd'hui, en particulier pour les systèmes de cryptographie basés sur des algorithmes classiques. Les ordinateurs quantiques exploitent les principes de la mécanique quantique pour effectuer des calculs de manière significativement plus rapide que les ordinateurs classiques, ce qui signifie qu'ils pourraient être capables de casser certains des algorithmes de chiffrement actuels.

En particulier, les ordinateurs quantiques pourraient menacer la sécurité des systèmes de chiffrement à clé publique basés sur des problèmes difficiles à résoudre pour les ordinateurs classiques, tels que l'algorithme RSA ou le chiffrement basé sur la courbe elliptique. Ces systèmes de cryptographie reposent sur l'arithmétique modulaire et la factorisation d'entiers, des problèmes qui deviendraient plus faciles à résoudre avec un ordinateur quantique suffisamment puissant.

Cependant, il est important de noter que le développement d'ordinateurs quantiques capables de casser ces algorithmes n'en est encore qu'à ses débuts, et il existe des défis techniques importants à relever pour construire des ordinateurs quantiques de grande taille et stables. De plus, des efforts sont en cours pour développer de nouvelles méthodes de cryptographie résistantes aux ordinateurs quantiques, telles que la cryptographie post-quantique.

Jean-Jacques Quisquater nous dira ce qu'il en pense.

Gérard

:

Lundi de la Cybersécurité de décembre

lundi 11 décembre 18h-20h

Renaud Lifchitz -expert cybersécurité – Holiseum

Les mots de passe sont-ils obsolètes ? Les alternatives pour un avenir sécurisé