Partenaires de l'ARCSI

BnF

ANSSI

CNIL.

orange

THALES

CAP'TRONIC

THEGREENBOW

G·ECHO
sécurité des systèmes d'information

HS2
Hervé Schauer Sécurité

Citalid

quarkslab
SECURING EVERY BIT OF YOUR DATA

Global Security Mag

MAG SECURS
INFORMATIQUE RESEAUX TELECOM INTERNET

1928 - 2018
90e anniversaire

12es Rencontres de l'ARCSI

La cryptologie, de la Grande Guerre au post-quantique

Jeudi 8 novembre 2018

BNF - Avenue de France - 75013 Paris

ARCSI

Association régie par la loi de 1901, reconnue d'intérêt général

SIRET : 511 069 569 00016
https://www.arcsi.fr

Secrétariat de l'ARCSI
secretariat@arcsi.fr

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

Jeudi 8 novembre 2018

Les hommes on le sait, sont particulièrement inventifs lorsqu'il s'agit de s'entre-tuer. Les guerres sont en effet à l'origine de multiples progrès techniques dont heureusement certains trouvent une utilité une fois la paix retrouvée. La Grande Guerre, dont nous célébrons le centenaire de la fin, n'a pas échappé à la règle : dans le domaine de compétence de l'ARCSI, la cryptographie et certains moyens de télécommunication qu'elle est venue renforcer ont fait des bonds de géant. C'est ce que notre prochain colloque se propose de montrer.

Celui-ci est en effet pour l'ARCSI l'occasion de célébrer un double anniversaire : le centenaire de la victoire de 1918 à laquelle, on le sait peu, les cryptologues ont pris une part déterminante, et les 90 ans de notre association constituée en 1928 précisément par ces héros de l'ombre, soit 10 ans après leurs succès et alors que la nécessaire discrétion qui avait entouré leurs exploits avait déjà cédé la place à l'oubli… D'autres pays et surtout d'autres responsables politiques avaient su reconnaître ce qu'ils devaient à ce qui était en train de devenir la science du secret. Ils surent, quand la terre trembla de nouveau, lui donner rapidement les moyens leur permettant de vaincre. Ainsi fit Churchill à *Bletchley Park*. D'autres sauront s'en servir pour assurer leur domination sur la planète comme Snowden a pu le révéler.

Mais c'est aussi durant cette guerre de 1914-1918, comme cela sera présenté, que les grands principes régissant les systèmes cryptographiques énoncés par Kerckhoffs ont été vérifiés tandis qu'était inventé par Vernam le procédé du « masque jetable » ou des « clefs une fois », qu'apparurent les premières machines ENIGMA ou que fut mis en application le « saut de fréquence » inventé par Nicolas Tesla.

Et c'est parce que cette période peut être considérée comme le point de départ de la cryptographie moderne que ce colloque se propose également de passer en revue les évolutions que sont l'industrialisation de la cryptanalyse qui va accélérer le développement de l'informatique, la compression des signaux vocaux utilisée dans le téléphone sécurisé de Roosevelt intégrée dans tous nos joujoux d'aujourd'hui, la véritable histoire de l'invention des systèmes à clé publique, l'engouement actuel pour les « blockchains » ou encore la crainte que suscitent aujourd'hui les performances de nouveaux algorithmes de factorisation sans parler des très attendus et redoutés ordinateurs quantiques.

Tout cela sera abordé au cours de ce colloque exceptionnel par des experts de très grand talent. Avec une envie commune pour les intervenants : sortir des sentiers battus.

Venez nombreux, l'ARCSI sera heureuse de partager avec vous cette journée mêlant histoire et technologie du futur.

Jean-Louis Desvignes

Participation gratuite *(dans la mesure des places disponibles)*
Inscription obligatoire sur le site de l'ARCSI : https://www.arcsi.fr

La cryptologie, de la Grande Guerre au post-quantique

8 h 30 *Accueil*

9 h 00 Général (2s) Jean-Louis Desvignes [A] *(Président de l'ARCSI)*
M^me^ Isabelle le Masne de Chermont *(BNF)*
• Introduction

9 h 20 P^r^ Olivier Forcade *(Sorbonne Université)*
• Le contexte des télécommunications civiles et militaires au début du XX^e^ siècle et de la Grande Guerre

10 h 00 M. Philippe Guillot [A] *(Université Paris 8 Vincennes Saint-Denis)*
• Les grands succès et échecs de la cryptologie à l'aube du XX^e^ siècle

10 h 40 *Pause*

11 h 00 P^r^ Jean-Jacques Quisquater [A] *(Université catholique de Louvain)*
• Du chiffre manuel à la mécanisation

11 h 45 Table ronde animée par M. Hervé Lehning [A] *(Écrivain et journaliste scientifique)*
Intervenants : Olivier Forcade, Philippe Guillot [A], Jean-Jacques Quisquater [A]
• De l'ingénieur au mathématicien

12 h 30 *Cocktail déjeunatoire*

14 h 00 M^me^ Marie-José Durand-Richard [A] *(Université Paris 8 Vincennes Saint-Denis)*
• La cryptanalyse dans la Seconde Guerre mondiale et son impact sur la naissance de l'informatique

14 h 40 M. Jean-Luc Moliner *(Groupe Orange)*
• Les deux faces de la cryptologie de masse

15 h 15 *Pause*

15 h 45 M. Philippe Duluc *(ATOS)*
P^r^ Jean-Jacques Quisquater [A]
• L'avenir plus ou moins proche : quantique, post-quantique et "cataCRYPT"

16 h 40 Table ronde animée par le P^r^ Sébastien-Yves Laurent *(Université de Bordeaux)*
Intervenants : ANSSI, CNIL, Jean-Louis Desvignes [A]
• Le dilemme sécurité/liberté

17 h 30 *Fin des Rencontres*

L'inventeur et collectionneur américain Jon Paul [A] présentera durant les pauses, dans l'espace Partenaires, une reconstitution du quantificateur du système SIGSALY ainsi qu'un micro simulateur d'ENIGMA.

[A] *Membre de l'ARCSI*
Questions/réponses possibles après chaque intervention