Conférence « Cryptographie post-quantique » à Pas Sage en Seine

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 juin 2018. Dernière mise à jour le 7 juillet 2018

https://www.bortzmeyer.org/pas-sage-en-seine-quantique.html

Le 29 juin, au festival Pas Sage en Seine <https://www.passageenseine.fr/>, j'ai eu le plaisir de faire un exposé technique sur la cryptographie post-quantique. Vu les progrès des calculateurs quantiques, faut-il jeter tout de suite les algorithmes classiques comme RSA ?

Voici les supports de l'exposé :

- Version adaptée à l'écran (en ligne sur https://www.bortzmeyer.org/files/pses2018-post-quantique-pdf),
- Version adaptée à l'impression sur des arbres morts (en ligne sur https://www.bortzmeyer.org/files/pses2018-post-quantique-PRINT.pdf),
- Source (en ligne sur https://www.bortzmeyer.org/files/pses2018-post-quantique.tex) en LaTeX/Beamer (format certainement le plus utilisé à Pas Sage en Seine).
- Sur la quantique, mais pas sur le calcul quantique, j'avais déjà fait un article sur une application de la cryptographie quantique <https://www.bortzmeyer.org/communication-quantique.html>.

La vidéo est en ligne, format WebM <http://data.passageenseine.org/2018/lapin-de-schrodinger_reflechissons-ensemble-cryptographie-post-quantique.webm> (et sur PeerTube <https://video.passageenseine.fr/videos/watch/c988e761-ad12-43aa-b99a-e5595ed90cb2>).

Les calculateurs quantiques utilisés, simulés ou réels :

- libquantum <http://www.libquantum.de/>, d'où venait le code `shor` utilisé sur un des transparents,
- Quintuple <https://www.github.com/corbett/QuantumComputing>,
- Et le vrai calculateur quantique d'IBM <https://quantumexperience.ng.bluemix.net/qx/experience>. Voir son excellente documentation <https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=beginners-guide&page=introduction>, ou l'exposé vidéo introductif de Talia Gershon <https://www.youtube.com/watch?v=S52rxZG-zi0&t=50s>. Depuis la rédaction de ces transparents, IBM propose également au public un ordinateur de 16 qubits.

Les logiciels post-quantiques utilisés :

- CodeCrypt <http://e-x-a.org/codecrypt>.

Il y avait **plein** d'autres trucs géniaux (comme d'habitude) à Pas Sage en Seine, n'hésitez pas à regarder le programme <https://programme.passageenseine.fr/>. Mes préférés (c'est complètement subjectif) : celui de Luckylex sur les lanceurs d'alerte, dénonçant la répression dont ils sont victimes, celui très concret de Nanar DeNanardon sur les innombrables traces numériques que nous laissons, avec plein de détails peu connus, comme le rôle de DHCP (cf. RFC 7819 [1] pour l'exposé du problème, et RFC 7844 pour une solution), l'exposé de David Legrand (Next Inpact) sur « 20 ans d[Caractère Unicode non montré [2]]évolution du numérique et de Next INpact », retraçant l'aventure d'un fanzine devenu un pilier de l'information libre sur le numérique (cf. leur dernier projet, La presse libre <https://beta.lapresselibre.fr/>), celui de Shaft « Un panda roux peut-il avoir une vie privée ? » montrant que Firefox a de sérieuses failles en matière de protection de la vie privée (mais les autres navigateurs sont pires), en partie parce que la Fondation Mozilla est trop proche des GAFA. Mais le meilleur exposé était celui de Suzanne Vergnolle et Benoît Piédallu sur leur projet « GDPRBookClub », un très intéressant projet de travail en commun sur le RGPD.

Sinon, sur les phénomènes quantiques, et notamment sur l'intrication, Marc Kaplan m'a fait découvrir cette excellente BD qui l'explique très bien <https://www.smbc-comics.com/comic/the-talk-3>, et avec humour.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7819.txt
2. Car trop difficile à faire afficher par LaTeX