RFC 6637 : Elliptic Curve Cryptography (ECC) in OpenPGP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 juin 2012

Date de publication du RFC : Juin 2012

https://www.bortzmeyer.org/6637.html

Le format OpenPGP, normalisé dans le RFC 4880 [1], permet de choisir parmi plusieurs algorithmes de cryptographie, afin de pouvoir suivre les progrès de la cryptanalyse. Notre tout nouveau RFC ajoute à la liste de ces algorithmes des algorithmes à courbes elliptiques, venant s'ajouter aux traditionnels RSA et DSA.

La section 3 rappelle deux ou trois choses sur les courbes elliptiques. Celles-ci sont décrites dans le RFC 6090 mais pour ceux et celles qui voudraient un cours plus scolaire, ce RFC recommande le Koblitz, « "*A course in number theory and cryptography*" », chapitre VI « "*Elliptic Curves*" » (ISBN : 0-387-96576-9, Springer-Verlag, 1987). La motivation principale pour utiliser les courbes elliptiques est qu'elles fournissent une alternative à l'augmentation régulière de la taille des clés RSA, augmentation rendue nécessaire par les avancées de la cryptanalyse. La section 13 de ce RFC fournit une estimation quantitative : la courbe elliptique P-256, avec ses 256 bits, fournit à peu près la résistance d'une clé RSA de 3 072 bits. Et la P-384 fournit environ l'équivalent de 7 680 bits RSA.

La NSA a listé une série d'algorithmes à courbes elliptiques recommandés, sous le nom de Suite B. Celle liste comprend deux algorithmes, ECDSA et ECDH, et trois courbes elliptiques (cf. norme NIST FIPS 186-3 <http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf>) P-256, P-384 et P-512. Ce RFC décrit donc comment intégrer la suite B au format ouvert et normalisé OpenPGP. Les deux algorithmes ont reçu les numéros <https://www.iana.org/assignments/pgp-parameters/pgp-parameters.xml#pgp-parameters-12> 19 (pour ECDSA) et 18 (pour ECDH).

Si vous voulez l'encodage exact des paramètres de la courbe elliptique dans les données, voir les sections 6 à 8 de notre RFC. L'encodage des clés cryptographiques figure en section 9.

Au moins deux mises en œuvre d'OpenPGP ont déjà du code pour ces courbes elliptiques, celle de Symantec et le logiciel libre GnuPG. Pour ce dernier, le code est déjà dans la version de développement (tête du dépôt git) mais pas encore dans la dernière version officiellement publiée (la 2.0.19).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4880.txt