RFC 8731 : Secure Shell (SSH) Key Exchange Method using Curve25519 and Curve448

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 février 2020

Date de publication du RFC : Février 2020

https://www.bortzmeyer.org/8731.html

Cela fait déjà pas mal de temps que des mises en œuvre du protocole SSH intègrent les courbes elliptiques « Bernstein », comme Curve25519. Ce RFC est donc juste une formalité, la normalisation officielle de cette utilisation.

SSH est normalisé dans le RFC 4251 [1]. C'est peut-être le protocole cryptographique de sécurisation d'un canal Internet le deuxième plus répandu, loin derrière TLS. Il permet de se connecter de manière sécurisée à une machine distante. En application du principe d'agilité cryptographique (RFC 7696), SSH n'est pas lié à un algorithme cryptographique particulier. Le protocole d'échange des clés, normalisé dans le RFC 4253, permet d'utiliser plusieurs algorithmes. Le RFC 5656 a étendu ces algorithmes aux courbes elliptiques.

Les courbes Curve25519 et Curve448, créées par Daniel Bernstein, sont décrites dans le RFC 7748. Depuis des années, elles s'imposent un peu partout, à la place des courbes NIST comme P-256. La libssh <https://www.libssh2.org/> a ces courbes depuis des années, sous l'ancien nom de curve25519-sha256@libssh Notre RFC ne fait qu'officialiser ces algorithmes, sous les nouveaux noms de curve25519-sha256 et curve448-sha512.

La section 3 du RFC décrit les détails de l'utilisation de ces algorithmes pour l'échange de clé. La méthode est proche de l'ECDH de la section 4 du RFC 5656.

Voici un exemple de session utilisant cet algorithme, avec OpenSSH 7.6 :

```
% ssh -v ...
...
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: curve25519-sha256
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4251.txt