TP: Hashing into Elliptic Curves

Jean-Sébastien Coron

Université du Luxembourg

1 SAGE

Download and install the Sage library [1].

2 NIST Curve P-192

The following elliptic-curve of equation:

$$E : y^2 = x^3 - 3x + b \mod p$$

is defined in [2], with:

$$\begin{aligned} p &= 6277101735386680763835789423207666416083908700390324961279 \\ n &= 6277101735386680763835789423176059013767194773182842284081 \\ b &= \texttt{0x64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1} \\ G_x &= \texttt{0x188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012} \\ G_y &= \texttt{0x07192b95ffc8da78631011ed6b24cdd573f977a11e794811} \end{aligned}$$

where n is the group order and $G = (G_x, G_y)$ is a generator of this group.

1. Verify that p is a prime and $p = 2 \mod 3$.

3 Icart's function

Implement Icart's hash function into the previous elliptic curve.

4 SPEKE

Implement the SPEKE protocol over the NIST curve P-192, using either Icart's function or SWU's algorithm.

References

1. Sage Mathematical Library, Available at `http://www.sagemath.org/`
2. FIPS PUB 186-3, *Digital Signature Standard (DSS)*. Available at `http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf`