

Secp256k1

Elliptic Curve Digital
Signature Algorithm
(**ECDSA**) based

refers to the
parameters of the
elliptic curve



used in Bitcoin's
public-key
cryptography

defined in *Standards for
Efficient Cryptography (SEC)*

special non-random way
which allows for especially
efficient computation

with the ECDSA algorithm

is often more than 30%
faster than other curves

