

# ECC - Elliptic-Curve Cryptography

Key Size	256 or 448 bits
Speed	<ul style="list-style-type: none"><li>~ factor of <math>10^6</math> cycles / operation</li><li>• Key generation: 1 - 5 ms (way faster than RSA)</li><li>• Encryption: 1 - 5 ms</li><li>• Decryption: 1 - 5 ms</li></ul>
Mathematical Foundation	Elliptic curves over finite fields

# Main ECC Standards

	secp256k1	curve25519	curve448
Year	2000	2005	2014
Inventor	Standards for Efficient Cryptography Group (SECG)	Daniel J. Bernstein	Mike Hamburg
Key Size	256	256	448
Applications	Bitcoin Ethereum	TLS, TOR Signal Protocol Monero, Zcash	TLS
Performances	+	++	+++