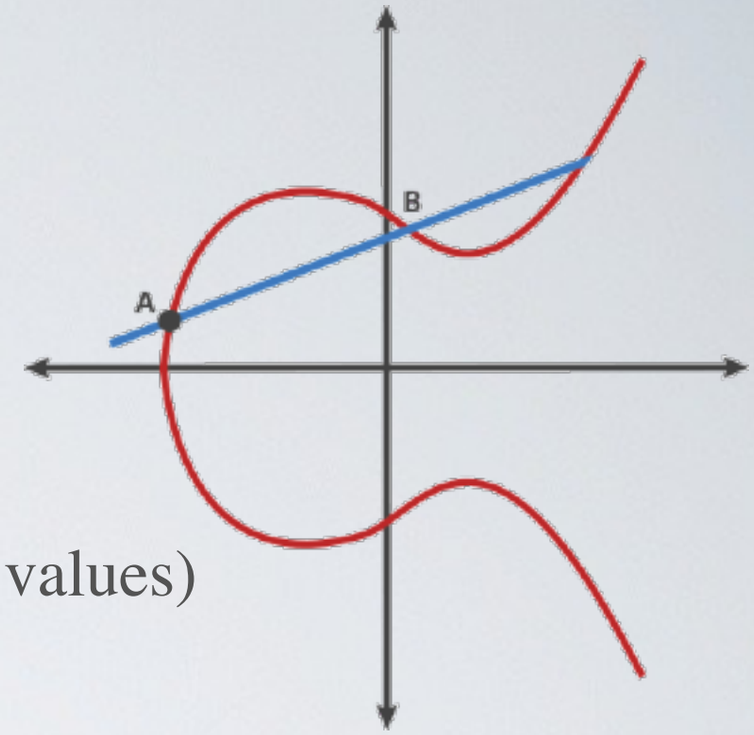
Main ECC Standards

	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	+	++	+++

Elliptic Curve Cryptography



Use Elliptic-curve for generating a cryptographic public-key pair
The algorithm is based on two public pieces:

- The curve equation $y^2 = x^3 + ax + b$ (a and b are fixed values)
- The generator point (fixed value)

When generating a key pair

1. the user "choose a random number" (within a given range) as private key
2. then derived the public key from the curve

✓ Smaller key sizes: 256 bits EC keys has the same entropy as RSA 3072 bits

✓ Can be used for digital signature (ECDSA algorithm)

✓ Can be used for key agreement (ECDH algorithm)

https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/