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

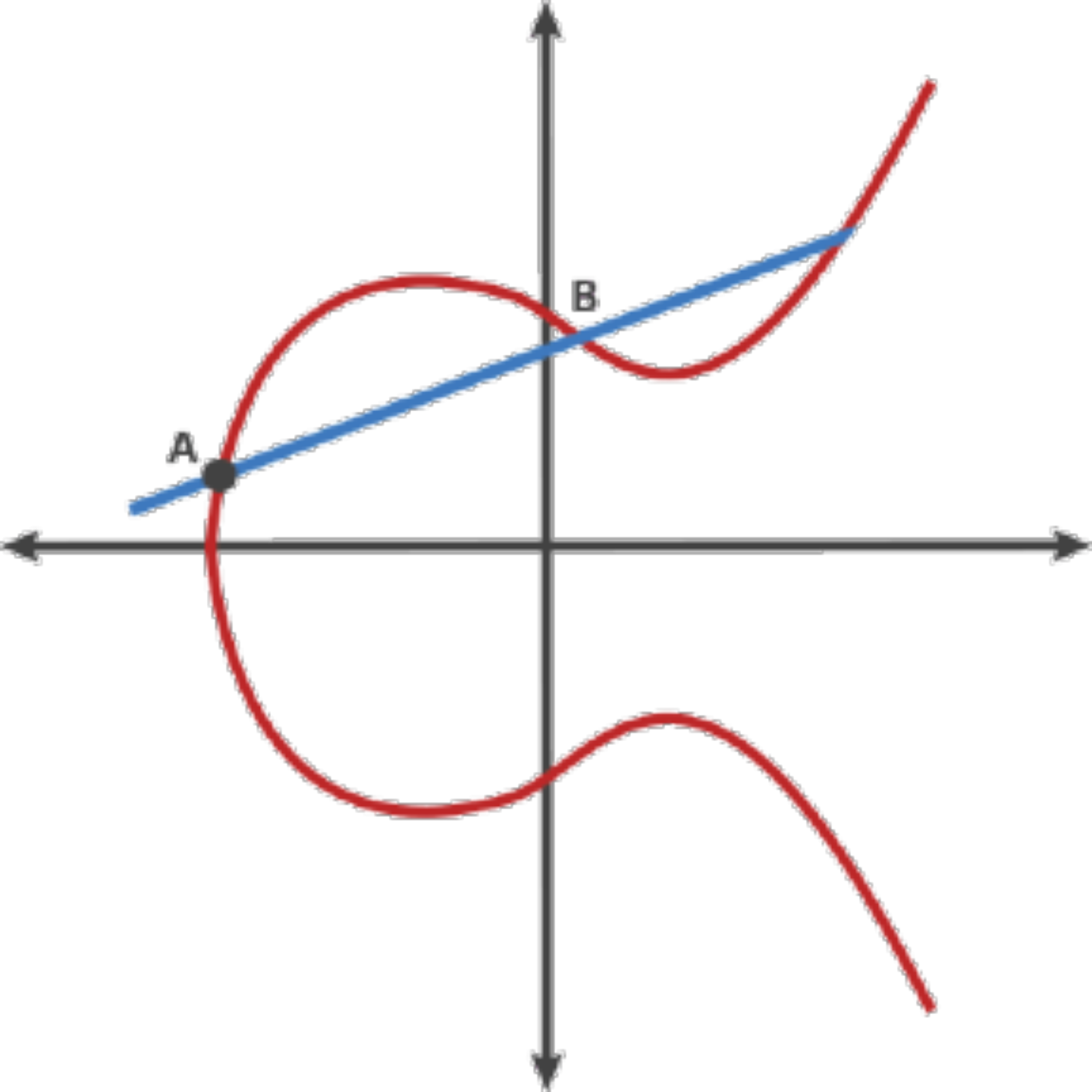
1. the user "choose a random number" (within a given range) as private key
2. then derived the public key from the curve

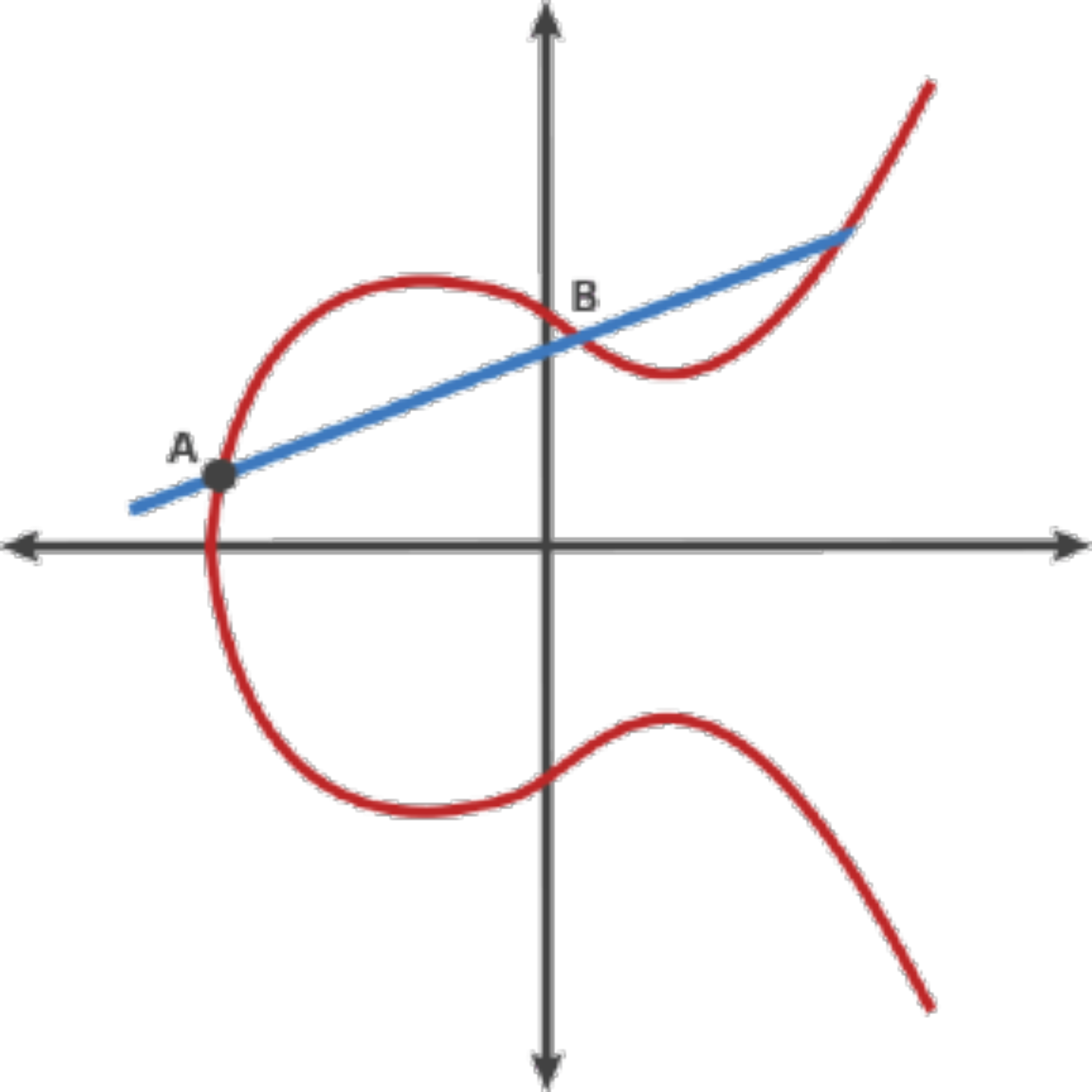
✓ Smaller key sizes: 256 bits EC keys has the same entropy as RSA 3072 bits

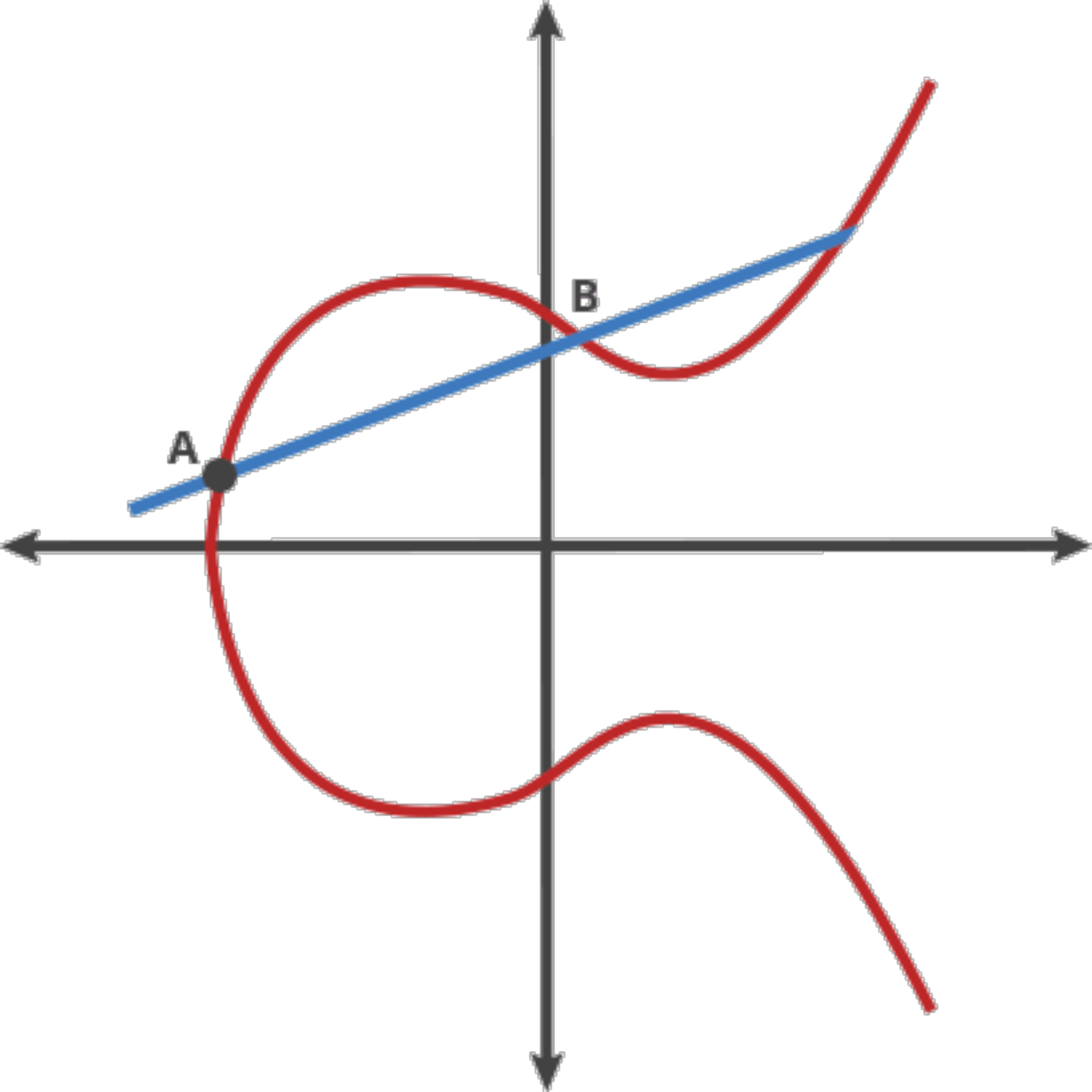
✓ Can be used for digital signature (ECDSA algorithm)

✓ Can be used for key agreement (ECDH algorithm)

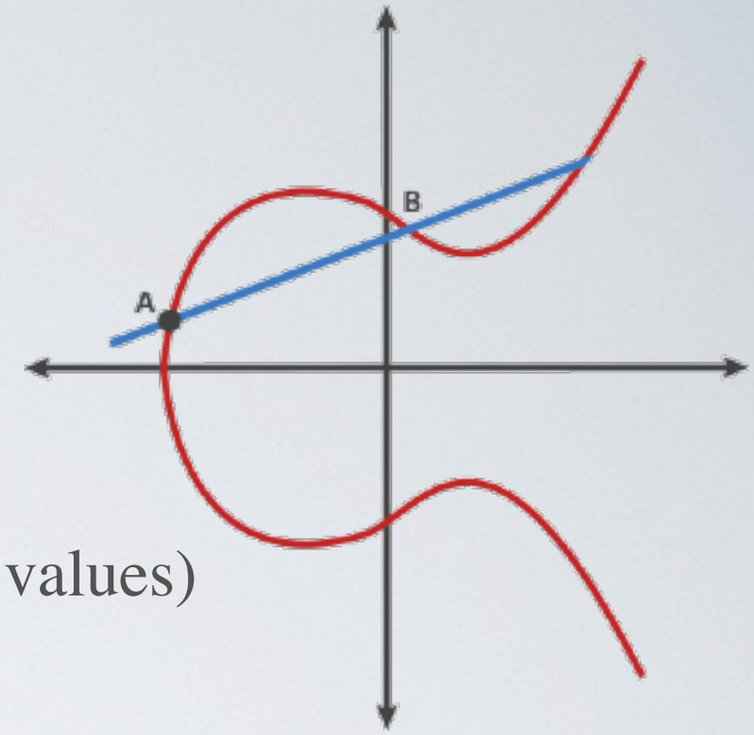
https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/


B
A


B
A


B
A

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/

Symmetric vs Asymmetric