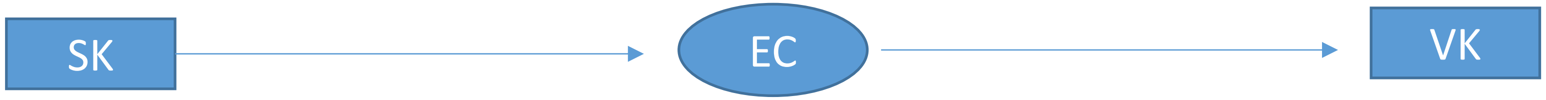
ECDSA

- Private key is a number called “signing key” (SK). It is secret.
- Public key is the “verification key” and is mathematically linked to the private key



Private key:
(number)

Elliptic curve operations:
Need base point, modulus, order

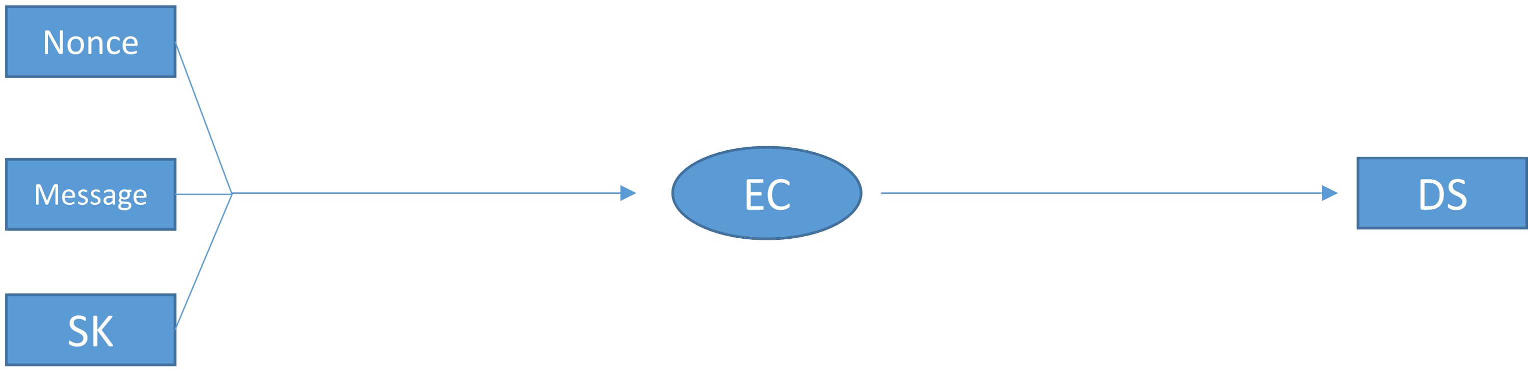
Public key:
coordinate (x, y)

Note: Easy to generate a public key with a private key. Not easy to go the other way.

ECDSA

- Digital signature

Nonce:
(random number)



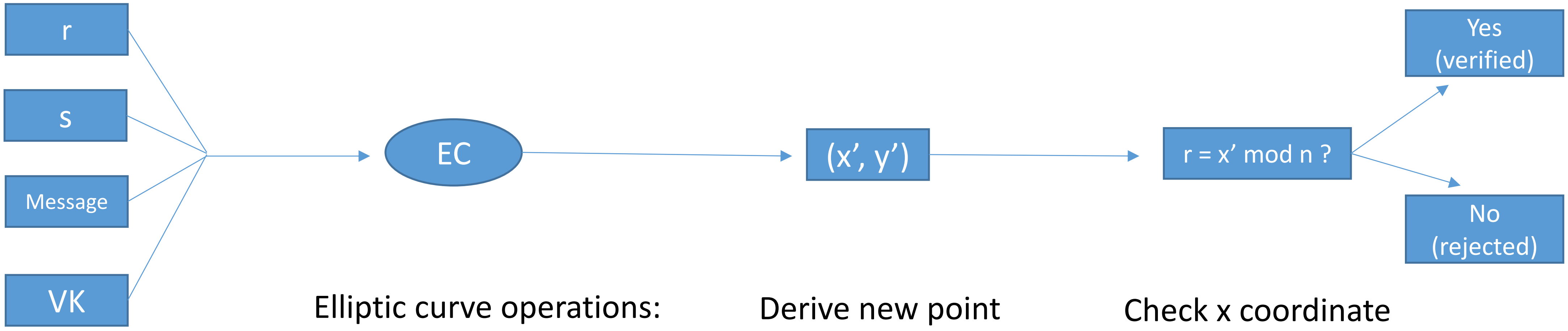
Private key:
(number)

Elliptic curve operations:
Need base point, modulus, order (n)

Digital signature:
coordinate (r, s)

ECDSA

- Verification



DS coordinates

r

s

Message

VK

EC

(x’, y’)

r = x’ mod n ?

Yes (verified)

No (rejected)

Elliptic curve operations: Need base point, order (n)

Derive new point on elliptic curve

Check x coordinate of new point and DS

Public key: (x, y)

Note r not used until verification step

How DSAs Work

Notice

- Proves that the person with the private key (that generated the public key) signed the message.
- Interestingly, digital signature is different from a usual signature in that it depends on the message, i.e., the signature is different for each different message.
- In practice, we do not sign the message, we sign a cryptographic hash of the message. This means that the size of the input is the same no matter how long the message is.