Deduce public key from signature

Zhao Yunke

May 28, 2022

1 ECDSA signing with private key d

Randomly select k, $R = kG = (x, y)$
$e = hash(m)$
$r = x \mod n, s = (e, rd_A)k^{-1} \mod n$
Signature(r,s)

2 Application of this deduce technique in ECDSA

$s = (e, rd_A)k^{-1} \mod n$
$e + rd_A = sk \mod n$
$d_A = r^{-1}(sk - e)$
$d_A G = r^{-1}(skG - eG)$
How to compute KG
$(kG)_x = x_1 = r \mod n$, then compute y_1
$e = hash(m)$ where m is not related public key