$P = d \cdot G$, $nG = I$

$Sig(d, m)$:

$k \in Z_n^*$, $R = kG$

$e = doublehash(m)$

$s = k^{-1}(e + dr) \bmod n$

$Sig = (r, s)$

$Verify(r, s)$:

$s^{-1}(hash(m) \cdot G + r \cdot P)$

其中 $s^{-1} = (k^{-1}(e+dr))^{-1} = (e+dr)^{-1} \cdot k$

原式 $= k(e+dr)^{-1}(e \cdot G + r \cdot d \cdot G)$

$= k(e+dr)^{-1}(e+dr) \cdot G$

$= kG$

$= R'$

forge:

$u, v \in F_n$

构造 $R' = (x', y') = uG + vP$

Verify时:

要让 $s'^{-1}(e'G + r'P) = R' = uG + vP$

只需 $\begin{cases} s'^{-1}e' \equiv u \bmod n \\ s'^{-1}r' \equiv v \bmod n \end{cases}$ 解 $\begin{cases} e' \equiv r'uv^{-1} \bmod n \\ s' \equiv r'v^{-1} \bmod n \end{cases}$

输出 $S' = (r', s')$ 作为签名，并提供 e 让别人验证

适用于不用提供 m，只提供 e 的情况，所以可以用 P 来通过 Verify