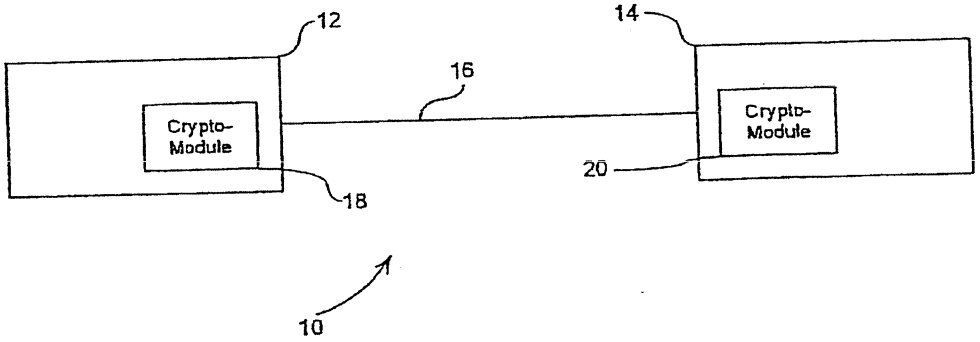

Figure 1

Signer 12	Verifier 14
generate (r, s) and m	
derive c	
substitute s with c	
$(r, c), m$ ⟶	$(r, c), m$
	compute $e = H(m)$
	compute $W = eP + rQ$
	$x = \log_W(cR)$
	$s = c\,l.x \bmod n$
	obtain (r, s) and verify if desired

Figure 2

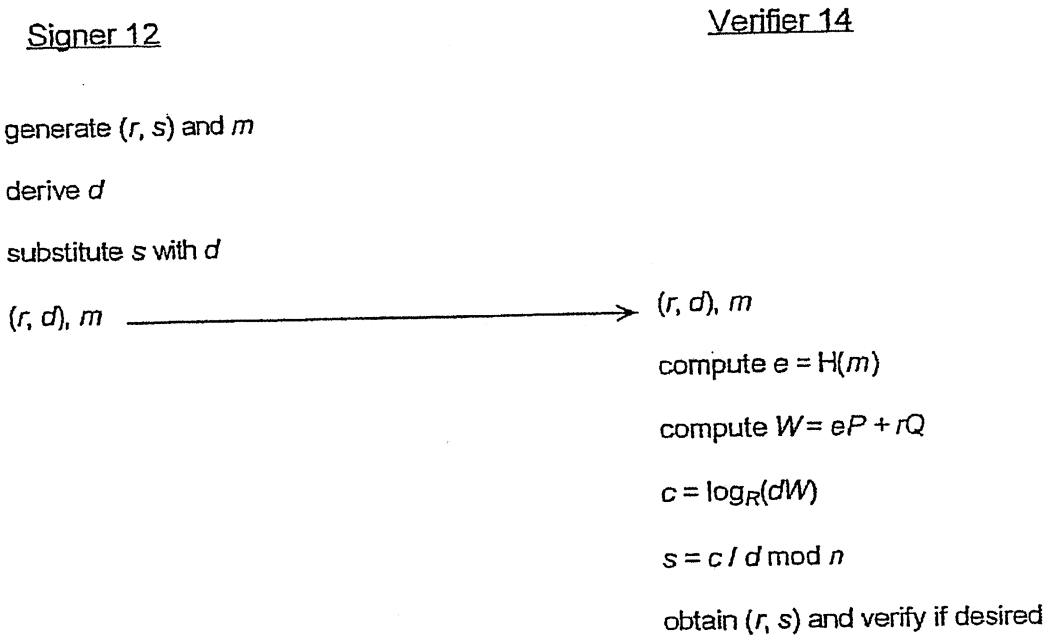
Signer 12
Verifier 14
generate (r, s) and m
derive d
substitute s with d
(r, d), m
(r, d), m
compute e = H(m)
compute W = eP + rQ
c = log_R(dW)
s = c / d mod n
obtain (r, s) and verify if desired

Figure 3