Blind Signature Raced on the RIA Scheme
Blind Signature Base
R=Mxbe 11 b# 15 blinding factor 11 19
Sb = Rd mod n
plane Fillixton (M) de veste
Signature (14) de se
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
S= Sbb-1 mod n (:: bt1 modh)
S=Md = 1 - CHEDT
S= Sbb-1 = Bdb-1= (Mxbe)db-1= Mdbedb-1= Mdbb=1
Chaum & van Antwerpen signature
Select prime p as p-1=29
$g^{k} \pmod{p}$ : $g = e^{(P-1)/q}$
Signing &
Q'E Ry 1
Signing &  graph  Samk (mod p)
Challenge: C= Sa(gk)b (mod p) . a, b is random
Response: $r = C^{k-1} = m^q gb \pmod{p}$ integers $r = C^{k-1} = m^q gb \pmod{p}$ $r = C^{k-1} = m^q gb \pmod{p}$
Test; 72 magb (modp)

disavoualit Protocol: Mila if test fails. A > R  $C1 = S^{a1}(g^k)^{b1} \mod p$ A checks whether r11= mangbl (mod p)
if yes, same process repeated cz = saz(gk) b2 (mod p) R+A: 72= C2k-1 821 = mangb2 (mod p). If yes, concludes that the signature is a Forgery if (r1g-b1) az = (r1g-b2) a1 (mad p)

paperism FLAT Date: / / Flat - Shamir Protocol Sclect PEq n=pxq (secret number) blu 1 & n-1 V = S2 modu the claimant random number'r' 0 to 4-1 X= 72 mod n y Select challenge 'C'

y = YSC  $y^2 = (75^c)^2 = 7^25^{2c} = 7^2(5^2)^c = XV^c$ Feige - Fiat - shamin Protocol private key [51,52,53