Blind Signature Based on the RSA Scheme

$B = M \times b^e$ // b is blinding factor

$S_b = B^d \bmod n$

Signature

$S = S_b b^{-1} \bmod n \quad (\because b^{-1} \bmod n)$

$S = M^d$

$S = S_b b^{-1} = B^d b^{-1} = (M \times b^e)^d b^{-1} = M^d b^{ed} b^{-1} = M^d b b^{-1} = M$

Chaum & van Antwerpen signature

Select prime p as $p-1 = 2q$

$g^k \pmod p \quad \therefore g = e^{(p-1)/q}$

Signing :

$g = e^{p-1}$

$s = m^k \pmod p$

Challenge : $c = s^a (g^k)^b \pmod p$ $\therefore$ a, b is random integers

Response : $r = c^{k^{-1}} = m^a g^b \pmod p$ $\because k^{-1} \bmod q$

Test : $r = m^a g^b \pmod p$

disavowal Protocol:

if test fails.

$A \rightarrow B$

$$c_1 = s^{a_1} (g^k)^{b_1} \bmod p$$

$B \rightarrow A$

$$r_1 = c_1^{k-1}$$

A checks whether $r_1 = m^{a_1} g^{b_1} \pmod p$

if yes, same process repeated

$A \rightarrow B$:

$$c_2 = s^{a_2} (g^k)^{b_2} \pmod p$$

$B \rightarrow A$:

$$r_2 = c_2^{k-1}$$

$r_2 = m^{a_2} g^{b_2} \pmod p$. If yes, concludes that the signature is a forgery

if $(r_1 g^{-b_1})^{a_2} = (r_1 g^{-b_2})^{a_1} \pmod p$

Fiat - Shamir Protocol

Select p & q

$n = p \times q$

(secret number) b/w 1 & n-1

$v = s^2 \bmod n$

the claimant

↳ random number 'r' 0 to n-1

$x = r^2 \bmod n$

↳ Select challenge 'c'

$y = rs^c$

$y^2 = (rs^c)^2 = r^2 s^{2c} = r^2(s^2)^c = xv^c$

Feige - Fiat - shamir Protocol

private key [s1, s2, s3