5. Podpis pierścieniowy (G_1,G_2,e,Pϵ G_1,H)

(G_1,G_2,e)- struktura dwuliniowa, G_1=E[n] + punkt P

H- funkcja haszująca H=$\{0,1\}^{\alpha}\rightarrow G_1$

B- grupa trzech użytkowników o kluczach:

Prywatnych $x_1,x_2,x_3 \epsilon Z_{11}$ i

Publicznych P=(2,3) $y_1= x_1P$, $y_2= x_2P$, $y_3=x_3P$

E_{11}: $y^2=(x^3-1)$

(σ_1, σ_2, σ_3), gdzie $\sigma_1=r_1P$, $\sigma_2=r_2P$, $\sigma_3=r_3P$

$G_1 = (H(m) - \sum_{i+1} g_i * r_i) * \frac{1}{x_1}$ (dla pierwszego członka grupy)

Zad.

Pokażemy, że zachodzi równość:

$$e(P, H(m)) = \sum_{i=1..3} (y_i, \sigma_i)$$

$$P = e(y_1, \sigma_1) * e(y_2, \sigma_2) * e(y_3, \sigma_3)$$

$$P = e\left(x_1, P, \left(\frac{H(m)}{\prod_{i\neq 1} e(y_i, \sigma_i)} \right)^{\frac{1}{x_1}} \right) * e\left(x_2P, r_2P\right) * e\left(x_3P, r_3P\right)$$

$$\downarrow$$

$$\left(\frac{H(m)}{e(y_2, \sigma_2) + e(y_3, \sigma_3)} \right)^{\frac{1}{x_1}} = \left(\frac{H(m)}{e(x_2, r_2) + e(x_3, r_3)} \right)^{\frac{1}{x_1}}$$

Podpis ślepy (autoryzacja bez względu w wiadomości)

1. Zaciemnienie wiadomości(czynnik losowy)
2. Podpis zaciemnionej wiadomości
3. Zdająca czynnika zaciemnionego

P- znane

x- klucz prywatny podpisującego

xP- klucz publiczny

1. x* H(m) – podpis pod m
2. zaciemnienie H(m)+ rP r- czynnik losowy
3. $\sigma=x(H(m)+ rP)$
4. Klient znosi zaciemnienie odejmując od σ wartość
   xrP= r(xP) xP- klucz publiczny