8.1 Ślepe podpisy cyfrowe w grupie GDH Diffe - Hallmana z luką

G_i – grupa DH z luką
$H – \{0,1\}^* \longrightarrow G_1$
(G_1,G_2,e) – struktura dwuliniowa
x – klucz prywatny podpisującego
$y = g^x$ – klucz publiczny, gdzie g to generator grupy

(zakładamy dla uproszczenia, że G_1 jest grupą multiplikatywną)

Schemat:

1 Faza

Zaciemnienie wiadomości m. Podmiot A przygotowuje wiadomość. Oblicza jej zaciemnienie czynnikiem losowym g^r i przekazuje do podpisu wartość $H(m)g^r$.

2 Faza

Podpisywanie:

Podmiot B wykonuje ślepy podpis $\sigma = (H(m)g^r)^{x^i}$ i przekazuje stronie A.

3 Faza

Obliczanie właściwego podpisu. Podmiot A zdejmuje czynnik zaciemniający obliczając:

$$\frac{\sigma}{g^r} = \frac{(H(m)g^r)^x}{g^{x_r}} = H(m)^x$$

8.2 Podpis skumulowany

Mamy grupę podpisujących różne wiadomości.

Cel:

Wykonanie podpisu pod wszystkimi wiadomościami takiego, żeby werfyfikacja była w jednym kroku.

x_i – klucze prywatne
$y_i = g^{xi}$ – klucze publiczne podpisujących (członków grupy)
m_i – wiadomość podpisywana przez i-tego członka

1. Podpisywanie

Każdy z członków oblicza podpis częściowy $\sigma_i H(m_i)^{x_i}$, który jest walidowany (sprawdzany) dzięki obliczaniu odpowiednich iloczynów Weila. Podpis całkowity ma postać:

$$\sigma = \prod \sigma_i$$

2. Weryfikacja podpisu

Podpis σ jest akceptowany wtedy i tylko wtedy gdy:

$$e(g,\sigma) = \prod_i e(y_i, H(m_i))$$

Wniosek:
Poprawność podpisu wynika z dwuliniowości iloczynu Weila, gdyż:

$$e(g,\sigma) = \prod_i e(g,\sigma_i) = \prod_i e(g, H(m_i)^{x_i}) =$$

$$\prod e(g, H(m_i))^{x_i} = \prod_i e(y_i, H(m))$$

8.3 Podpis pierścieniowy

Ten rodzaj podpisu pozwala na ukrycie tożsamości podpisującego. Wiadomo jedynie, że jest on członkiem danej grupy podpisujących (użytkowników w liczbie k).

1. Podpisywanie wiadomości m.
   Dowolny użytkownik używa swojego klucza prywatnego x_i i kluczy publicznych y_{ij} gdzie $i \neq j$ wszystkich pozostałych użytkowników do obliczenia podpisu pod wiadomością m.

   Pozostali użytkownicy nie biorą udziału w tym podpisywaniu. Podpisujący w przeciwieństwie do podpisów grupowych jest niewytrapialny.

Uzytkownik i-ty oblicza podpis generując najpierw losowe r_j dla wszystkich j $\neq$ i. Podpis ma postać:

$\sigma(m) = (\sigma_1(m),...,\sigma_k(m))$, gdzie $\sigma_j = g^{r_j}, (i \neq j)$,

$$\sigma_i = (\frac{H(m)}{\prod_{i \neq j} y_j^{r_j}})^{\frac{1}{x_i}}$$

2. Weryfikacja

Podpis $\sigma_1, \sigma_2, ..., \sigma_k$ jest zaakceptowany wtedy i tylko wtedy gdy

$$e(g, H(m)) = \prod_{s=1}^{k} e(y_i, \sigma_i)$$

<u>Wniosek:</u>

Poprawność wynika z własności iloczynu Weila, a mianowicie:

$$\prod_{s=1}^{k} e(y_s, \sigma_s) = \prod_{s \neq i} e(g^{x_s}, g^{r_s}) e(g^{x_i}, (\frac{H(m)}{\prod_{j \neq i} y_j^{r_j}})^{\frac{1}{x_i}}) =$$

$$\prod_{s \neq i} e(g, g^{x_s r_s}) e(g, \frac{H(m)}{\prod_{j \neq i} y_j^{r_j}}) = \prod_{s \neq i} e(g, y_s^{r_s} \cdot \frac{H(m)}{\prod_{j \neq i} y_j^{r_j}}) =$$

$$e(g, \prod_{s \neq i} (\frac{y_s^{r_s}}{\prod_{j \neq i} y_j^{r_j}}) H(m) = e(g, 1 * H(m))$$

c.n.d