

## 1 Uwagi:

Jako oznaczenie współrzędnej w  $n$ -tym wymiarze jest użyta notacja taka jak do ciągów  $(m_n)$ .

Niezależnie od wyboru wiadomości da się skonstruować  $l$  wymiarową hipers-

fere o takim promieniu  $(\sqrt{\sum_{i=0}^l m_i^2})$  by punkt  $m$  leżał na niej.

Szyfrowanie zadziała jeśli  $\exists n(p_n \bmod k \neq m_n)$ .

## 2 Wyprowadzenie $t$ ze wzoru:

$m$  - punkt leżący na hipersferze

$p$  - punkt przez który i przez  $m$  zostanie przeprowadzona prosta, której będą wyliczone wspólnepunkty z hipersferą.

$k$  - liczba wymiarów przestrzeni, w której jest punkt  $p$

$l$  - liczba wymiarów hipersfery

$$\begin{aligned}
 \sum_{i=0}^l (m_i + t(p_i \bmod k - m_i))^2 &= \sum_{i=0}^l m_i^2 & / - \sum_{i=0}^l m_i^2 \\
 \sum_{i=0}^l (m_i + t(p_i \bmod k - m_i))^2 - \sum_{i=0}^l m_i^2 &= 0 \\
 \sum_{i=0}^l (m_i^2 + 2m_i t(p_i \bmod k - m_i) + t^2(p_i \bmod k - m_i)^2) - \sum_{i=0}^l m_i^2 &= 0 \\
 \sum_{i=0}^l (2m_i t(p_i \bmod k - m_i) + t^2(p_i \bmod k - m_i)^2) &= 0 & / : t \\
 \sum_{i=0}^l (2m_i(p_i \bmod k - m_i) + t(p_i \bmod k - m_i)^2) &= 0 & / - \sum_{i=0}^l (2m_i(p_i \bmod k - m_i)) \\
 - 2 \sum_{i=0}^l m_i(p_i \bmod k - m_i) &= t \sum_{i=0}^l (p_i \bmod k - m_i)^2 & / : \sum_{i=0}^l (p_i \bmod k - m_i)^2 \\
 t &= -2 \frac{\sum_{i=0}^l m_i(p_i \bmod k - m_i)}{\sum_{i=0}^l (p_i \bmod k - m_i)^2}
 \end{aligned}$$

### 3 Szyfrowanie:

Do reszt z dzielenia dodawane jest  $w_n \bmod k$  na wypadek, gdy  $a_n = 0$  i by zamaskować promień hipersfery.

Wejście:

m - wiadomość

p - pierwsza część klucza

w - druga część klucza

k - długość pierwszej części klucza

d - długość drugiej części klucza

l - indeks ostatniego elementu wiadomości

Wyjście:

q - zaszyfrowana wiadomość

b - mianownik do użycia przy odszyfrowywaniu

$$a_n = p_n \bmod k - m_n$$

$$b = \sum_{i=0}^l a_i^2$$

$$c = 2 \sum_{i=0}^l m_i a_i$$

$$e_n = b m_n - a_n c$$

$$q_{n_0} = \lfloor \frac{e_n}{b} \rfloor$$

$$q_{n_1} = e_n \bmod b + w_n \bmod d$$

## 4 Odszyfrowywanie:

Wejście:

q - zaszyfrowana wiadomość

b - mianownik do użycia przy odszyfrowywaniu

p - pierwsza część klucza

w - druga część klucza

k - długość pierwszej części klucza

d - długość drugiej części klucza

l - indeks ostatniego elementu zaszyfrowanej wiadomości

Wyjście:

m - wiadomość

$$e_n = bq_{n_0} + q_{n_1} - w_n \bmod d$$

$$f_n = bp_{n \bmod k} - e_n$$

$$g = \sum_{i=0}^l f_i^2$$

$$h = 2 \sum_{i=0}^l e_i f_i$$

$$d = gb$$

$$m_n = \frac{ge_n - f_n h}{d}$$