# 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 hipersferę 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 - wektor kierunkowy prostej przechodzącej przez punkt $m$

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

l - liczba wymiarów hipersfery leżącej w l+1 wymiarowej przestrzeni

$$\sum_{i=0}^{l}(m_i + tp_{i \bmod k})^2 = \sum_{i=0}^{l} m_i^2 \qquad / - \sum_{i=0}^{l} m_i^2$$
$$\sum_{i=0}^{l}(2m_i tp_{i \bmod k} + t^2 p_{i \bmod k}^2) = 0 \qquad / : t$$
$$\sum_{i=0}^{l}(2m_i p_{i \bmod k} + tp_{i \bmod k}^2) = 0 \qquad / - \sum_{i=0}^{l} 2m_i p_{i \bmod k}$$
$$-2\sum_{i=0}^{l} m_i p_{i \bmod k} = t\sum_{i=0}^{l} p_{i \bmod k}^2 \qquad / : \sum_{i=0}^{l} p_{i \bmod k}^2$$
$$t = -2\frac{\sum_{i=0}^{l} m_i p_{i \bmod k}}{\sum_{i=0}^{l} p_{i \bmod k}^2}$$

## 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 - wiadmość
- 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

$b = \sum\limits_{i=0}^{l} p_{i \bmod k}^2$
$c = 2 \sum\limits_{i=0}^{l} m_i p_{i \bmod k}$
$e_n = bm_n - cp_{n \bmod k}$
$q_{n_0} = \lfloor \frac{e_n}{b} \rfloor$
$q_{n_1} = e_n - bq_{n_0} + w_{n \bmod d}$

## 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 - wiadmość

$e_n = bq_{n_0} + q_{n_1} - w_{n \bmod d}$
$f_n = bp_{n \bmod k}$
$g = \sum\limits_{i=0}^{l} f_i^2$
$h = 2\sum\limits_{i=0}^{l} e_i f_i$
$o = gb$
$m_n = \frac{ge_n - f_n h}{o}$