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 $(\sqrt{\sum\limits_{i=0}^{l} m_i^2})$ 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 na drugi koniec hipersfery - zostanie obliczony punkt wspólny hipersfery i prostej.

k - liczba wymiarów przestrzeni, w której jest punkt p

l - indeks ostatniego wymiaru hipersfery

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

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

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

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

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

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

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

3 Szyfrowanie jako punkt wspólny l wymiarowej hipersfery o promieniu $\sqrt{\sum_{i=0}^{l} m_i^2}$ i prostej przechodzącej przez punkty p i m:

Punkt m w rezultacie długości promienia leży na hipersferze. Dzielenie e_n przez b zostanie pominięte i wykonane będzie dopiero przy odszyfrowywaniu, kiedy wiadomo będzie, że dzielenie odwróci wynik (zwróci z powrotem wiadomość), więc będzie on na pewno całkowity.
Przy liczeniu e_n dodawane jest do wyniku $p_{n \bmod k} \bmod k$ chociaż nie ma tego we wzorach, żeby zamaskować wynik właściwego działania względnie niewielką liczbą na wypadek, gdy $a_n = 0$.
Wejście:

m - wiadmość

p - klucz

k - długość klucza

l - indeks ostatniego elementu wiadomości

Wyjście:

e - zaszyfrowana wiadmość

b - mianownik do użycia przy odszyfrowywaniu

$a_n = p_{n \bmod k} - m_n$
$b = \sum_{i=0}^{l} a_i^2$
$c = 2 \sum_{i=0}^{l} m_i a_i$
$e_n = bm_n - a_n c + p_{n \bmod k} \bmod k$

4 Odszyfrowywanie jako przeprowadzenie prostej przez punkty $\frac{e_n}{b}$ i p z powrotem do punktu m (na drugi koniec l wymiarowej hipersfery względem $\frac{e_n}{b}$), którym jest wiadmość:

Punkt m w rezultacie długości promienia leży na hipersferze, a $\frac{e_n}{b}$ jest punktem wspólnym prostej i hipersfery, więc też leży na hipersferze.
Wejście:

e - zaszyfrowana wiadmość

b - mianownik do użycia przy odszyfrowywaniu

p - klucz

k - długość klucza

l - indeks ostatniego elementu zaszyfrowanej wiadomości

Wyjście:

m - wiadmość

$q_n = e_n - p_{n \bmod k} \bmod k$
$f_n = bp_{n \bmod k} - q_n$
$g = \sum\limits_{i=0}^{l} f_i^2$
$h = 2 \sum\limits_{i=0}^{l} q_i f_i$
$d = gb$
$m_n = \frac{gq_n - f_n h}{d}$