Ежегодная международная научно-практическая конференция
«РусКрипто'2020»

Обобщенные (L,G)-коды в современном алгоритме Нидеррайтера

Беззатеев С.В.
bsv@aanet.ru
зав. кафедрой технологий защиты информации,
Санкт Петербургский университет аэрокосмического приборостроения

План доклада

- Классические(рациональные) коды Гоппы (1970)
- Алгоритмы Мак Элиса(1978) и Нидеррайтера (1986)
- Современный вариант алгоритма Ниддерайтера/Мак Элиса
- Обобщенные (L,G)- коды
- Использование обобщенных (L,G) –кодов в современном алгоритме Ниддерайтера

Классические(рациональные) коды Гоппы

В. Д. Гоппа, Новый класс линейных корректирующих кодов, Пробл. передачи информ., 6:3 (1970), 24–30;

Определение 1. Двоичный вектор **a**=($a_1a_2...a_n$) является кодовым словом кода Гоппы тогда и только тогда, когда выполняется следующее сравнение

$$\sum_{i=1}^{n} a_i \frac{1}{x-\alpha_i} \equiv 0 \ mod \ G(x) \quad , \alpha_i \in GF(2^m), n \leq 2^m, G(x) \in F_{2^m}[x], \deg G(x) = t \qquad (1)$$

Определение 2. Код Гоппы называется сепарабельным если G(x) – сепарабельный многочлен.

Определение 3. Код Гоппы называется неприводимым если G(x) – неприводимый многочлен.

Утверждение 1. Сепарабельный двоичный код Гоппы имеет избыточность *r* и минимальное расстояние *d*, определяемые следующими неравенствами

$$r \leq mt, \quad d \geq 2t + 1$$

Проверочная и порождающая матрица кода

$$\mathrm{H} = \begin{bmatrix} \frac{1}{G(\alpha_1)} & \cdots & \frac{1}{G(\alpha_n)} \\ \vdots & \ddots & \vdots \\ \frac{\alpha_1^{t-1}}{G(\alpha_1)} & \cdots & \frac{\alpha_n^{t-1}}{G(\alpha_n)} \end{bmatrix}, \alpha_i \in GF(2^m),\ n \le 2^m,\ G(x) \in F_{2^m}[x],\ \deg G(x) = t \qquad (2)$$

$H_{[r \times n]} = [I \quad \hat{H}]$, r ≤ mt

$G_{[k \times n]} = [\hat{H}^T \quad \vec{I}]$, k ≥ n - mt

Алгоритмы Мак Элиса и Нидеррайтера

R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical report, NASA, 1978
H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory, 15(2):159-166, 1986.

Секретный ключ

G(x)→ H→ G , A – не сингулярная матрица [k x k] ,
P – перестановочная матрица [n x n]

G(x) → H , A – не сингулярная матрица [r x r] ,
P – перестановочная матрица [n x n]

Открытый ключ

PK= A·G·P

PK= A·H·P

Шифрование

m·PK + e = b , wt(e)=t

PK·m^T = s , wt(m)=t

Расшифрование

b· P^{-1}=m·A·G + e·P^{-1},
s’ = b· $P^{-1}\cdot H^T$=m·A·G·H^T + e·$P^{-1}\cdot H^T$=e·$P^{-1}\cdot H^T$

$s' = A^{-1}$·s =H·P·m^T

*Нахождение вектора ошибки **e’** по синдрому s’ при известном G(x)*

e’=e·P^{-1} , e=e’ ·P^{-1}

e’=P·m^T , $m^T = P^{-1}$·e’

Современный вариант алгоритма Ниддерайтера/Мак Элиса

D. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, and W. Wang, Classic McEliece: conservative code-based cryptography, 2019 .https://classic.mceliece.org/nist/mceliece-20190331.pdf

Секретный ключ G(x)

Открытый ключ PK= $\widehat{H}$ G(x)→ H $\underset{[r \times n]}{\rightarrow}$ $\underset{[r \times k]}{\widehat{H}}$, $H = [I \quad \widehat{H}]$

Шифрование **e → C , K** $[I \quad \widehat{H}] \cdot e^T = C_0$, wt(e)=t , C_1 = Hash(2,e) , **C= (C_0, C_1) , K = H(1, e, C);** (K – сеансовый ключ)

Расшифрование **C_0 → e** $[C_0 \quad \hat{0}] = a \oplus e$, a – кодовое слово кода Гоппы с многочленом G(x)

*Нахождение вектора ошибки **e** при известном G(x)*

Обобщенные (L,G)- коды

S.V.Bezzateev, N.A Shekhunova, One generalization of Goppa codes , Proceedings of ISIT-97, p.299, Ulm, Germany, 1997, p.299

Определение 4. Множество нумераторов позиций L определяется как множество рациональных функций :

$$L = \left\{ \frac{f'_1(x)}{f_1(x)}, \frac{f'_2(x)}{f_2(x)}, \dots, \frac{f'_n(x)}{f_n(x)} \right\},$$

где $f'_i(x)$ – формальная производная знаменателя $f_i(x)$ и

$f_i(x) = x^{l_i} + c_{l_i-1,i}x^{l_i-1} + \cdots c_{1,i}x + c_{0,i}$, $c_{j,i} \in GF(2^m)$, $c_{0,i}$, $c_{j,i} \in GF(2^m)$, $(f_i(x),f_j(x))=1$, $(f_i(x),G(x))=1, \forall i,j,\ i \neq j$, *deg* $G(x)=t$

Определение 5. Двоичный вектор **a**=$(a_1a_2...a_n)$ является кодовым словом обобщенного (L,G)-кода тогда и только тогда, когда выполняется следующее сравнение

$$\sum_{i=1}^{n} a_i \frac{f'_i(x)}{f_i(x)} \equiv 0 \ mod\ G(x) \quad (3)$$

Утверждение 2. Сепарабельный двоичный код Гоппы имеет избыточность r и минимальное расстояние d, определяемые следующими неравенствами

$$r \leq tm\ ,\ d_G \geq \frac{2t+1}{l}\ ,\ l = \max l_i$$

Проверочная и порождающая матрица кода

$$\frac{f'_i(x)}{f_i(x)} \equiv s_i(x) \equiv b_{i,t-1}x^{t-1} + b_{i,t-2}x^{t-2} + \cdots . + b_{i,1}x^1 + b_{i,0} \ mod\ G(x),\ G(x) \in F_{2^m}[x], \deg G(x) = t\ , b_{i,j} \in GF(2^m)$$

$$H = \begin{bmatrix} b_{1,t-1} & b_{2,t-1} & \cdots & b_{n,t-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{1,0} & b_{2,0} & \cdots & b_{n,0} \end{bmatrix},\ n \leq \sum_{i=1}^{r} I_{2^m}(i),$$

где $I_{2^m}(i)$ – число неприводимых многочленов степени i с коэффициентами из $GF(2^m)$

$$\underset{[r \times n]}{H} = [I \quad \hat{H}] \quad , r \leq mt$$

$$\underset{[k \times n]}{G} = [\hat{H}^T \quad \vec{I}] \quad , k \geq n - mt$$

Пример обобщенного (L,G)- кода

Пусть m=6 , GF(2^6) и l =2. Тогда $I_{2^6}(1) = 64$, $I_{2^6}(2) = \frac{2^{12}-2^6}{2}$, n=2016+64=2080.

$G(x) \in F_{2^6}[x]$, $\deg G(x) = 60$,

Тогда d≥61 и число информационных символов k≥2080 - 60·6=1720. Классический код Гоппы с такой же длиной потребует использования в качестве нумераторов позиций все элементы поля GF(2^{11}) с удлинением на 32 позиции или можно использовать укороченный код с нумераторами из GF(2^{12}).

Анализ безопасности

Обобщенные (L,G) – коды

$deg\ f_i(x) \leq 2,\ f_i(x) \in F_{2^7}[x]$

t= 29 r= 406 k= 7850 n=8256 security= 128 size PK= 398387 byte

t= 56 r= 784 k= 7472 n=8256 security= 193 size PK= 732256 byte

t= 97 r= 1358 k= 6898 n=8256 security= 256 size PK=1170935 byte

Классические коды Гоппы

$deg\ f_i(x) = 1,\ f_i(x) \in F_{2^{13}}[x]$

t= 28 r= 364 k= 7828 n= 8192 security= 127 size PK= 356174 byte

t= 53 r= 689 k= 7503 n= 8192 security= 192 size PK= 646195 byte

t= 90 r= 1170 k= 7022 n= 8192 security= 256 size PK= 1026967 byte

Вопросы

Контактная информация

Электронная почта:

bsv@aanet.ru

Телефон:

+7 904 517-09-51

Сайт:

www. guap.ru