УДК 658.518.3

Ю.А. Тарнавський, І.О. Шарапов, М.В. Колоскова

Національний технічний університет України «Київський політехнічний інститут», Київ

РЕАЛІЗАЦІЯ ОПЕРАЦІЙ АРИФМЕТИКИ ПО МОДУЛЮ ДВА В ПОЛІНОМІАЛЬНОМУ МЕТОДІ ШИФРУВАННЯ

Розглянуто поліноміальний метод шифрування, реалізація якого вимагає ефективної організації операцій над поліномами. Розроблено бібліотеку класів з методом для виконання таких операцій.

Ключові слова: криптографія, кодування, арифметика по модулю два, програмування

Постановка проблеми

В теорії кодування добре відомі методи циклічного кодування. Такі методи забезпечують передавання даних з необхідною достовірністю і використовуються в системах промислової автоматизації, радіоінтерфейсах, кодексах відеопослідовностей, шинах передачі даних процесорів. Проте циклічні коди можуть використовуватись і в якості основи криптографічних систем, які допускають просту апаратну реалізацію. В цій роботі моделюється функціонування такої системи.

Аналіз останніх досліджень і публікацій

Основні способи опису циклічних кодів та їх застосування в методах кодування розглядаються в роботах багатьох вітчизняних і зарубіжних авторів [3-8]. Робота над удосконаленнями цих методів і підвищення ефективності використовуваних в них алгоритмів продовжується [1].

Формулювання мети статті

Метою роботи є розробка ефективної програмної реалізації операцій в поліноміальному методі шифрування.

Виклад основного матеріалу

Поліноміальний метод шифрування ґрунтується на підходах, запозичених з теорії кодування. Математичною основою створення і використання циклічних кодів є арифметика по модулю два. В ній числа представляють у вигляді полінома над простим полем ГалуаGF (2):система числення замінюється деякою фіктивною змінною x, степінь якої відповідає номеру розряду числа, а коефіцієнт - значенням самого розряду. Так, поліноміальним представленням двійкового числа $10101=1\cdot2^4+0\cdot2^3+1\cdot2^2+0\cdot2^1+1\cdot2^0$ є поліном $P(x)=x^4+x^2+1$.

Будь-який код можна записати у вигляді матриці з k лінійно незалежних рядків, кожний з яких містить n символів. Особливе значення в арифметиці по модулю два відіграють так звані циклічні коди, у яких рядки твірної матриці пов’язані додатковою умовою циклічності: всі рядки матриці можуть бути отримані в результаті циклічного зсуву однієї (твірної) комбінації. Так, у випадку n=5, твірна матриця циклічного коду має вигляд:

$$\begin{pmatrix} 10101 \\ 11010 \\ 01101 \\ 10110 \\ 01011 \end{pmatrix}$$

Поліноменальні представлення кодових (n-1)-послідовностей циклічного коду є елементами розширення простого поля GF (2^n) з коефіцієнтами з основного поля GF(2). Їх додавання проводиться за правилами основного поля, тобто - по модулю два. Правило множення в розширенні поля аналогічно правилу множення многочленів з подальшим зведенням по модулю деякого спеціального полінома, щоб операції залишались оберненими (інакше елементи не утворять поле). Такий поліном має бути таким, що не зводиться в полі GF (2), тобто його не можна розкласти на множники, використовуючи тільки многочлени з коефіцієнтами з поля GF(2).

На сьогодні не існує систематичного способу пошуку поліномів, що не зводиться в полі GF (2) . Таблиця деяких з таких поліномів наведена в [2]: x^2+x+1, x^3+x+1, x^3+x+1, x^5+x^2+1, x^6+x+1, x^7+x^3+1, $x^8+x^4+x^2+x^3+1$, x^9+x^4+1, $x^{10}+x^3+1$ та ін.

За поліноміальним методом шифрування в якості ключа використовується поліном, що не

зводиться. Поліноміальне шифрування ґрунтується на використанні операцій множення і ділення по модулю на поліном, що не зводиться.

Операція множення поліномів по модулю відрізняється від звичайної операції множення поліномів способом обчислення коефіцієнтів при степенях:

- коефіцієнти, що додаються, переводяться в двійкове представлення і додаються по модулю два (операція XOR);
- коефіцієнти, що множаться, переводяться в двійкове представлення, цифри розрядів множаться за звичайними правилами, а сумування виконується по модулю два.

Операція ділення поліномів по модулю виконується аналогічно звичайній операції ділення поліномів, але обчислення коефіцієнтів при степенях здійснюється за наведеними правилами. Для швидкого виконання обчислень можуть використовуватись відповідні таблиці додавання і множення, що будуються на основі вказаних правил.

В поліноміальному методі шифрування символи відкритого повідомлення спочатку переводяться в цифри за порядковим номером в алфавіті, потім повідомлення зводиться до поліноміального вигляду, в якому отримані цифри розглядаються як коефіцієнти поліному. Отриманий поліном множиться по модулю на завчасно вибраний поліном, що не зводиться, в результаті чого одержується криптоном. Далі з коефіцієнтів криптоному утворюється цифрове представлення зашифрованого повідомлення, з якого шляхом заміни цифр на символи алфавіту отримується криптограма.

Для розшифрування символи криптограми переводяться в цифри за порядковим номером в алфавіті, після чого вона зводиться до поліноміального вигляду. Поліноміальне представлення криптограми ділиться по модулю на поліном-ключ. У разі правильного виконання попередніх операцій ділення має виконуватись без залишку. З коефіцієнтів отриманого поліному утворюється цифрове представлення вхідного повідомлення, з якого шляхом заміни цифр на символи алфавіту отримується вхідне повідомлення.

Для практичного використання операцій поліноміальної арифметики в криптографічних алгоритмах нами реалізована статична бібліотека класів для платформи. NET, що містить метод множення по модулю два.

Реалізація функції множення

Дана функція реалізована в бібліотеці polynomialMethods.dll. Вона має назву AbsMuli приймає значення firstValue tasecondValue типу double, а також symbolsInAlphabet типу integer. Параметр firstValue відповідає за значення першого множника, параметр secondValue за значення другого множника, а параметр symbolsInAlphabet приймає значення кількості символів в користувацькому алфавіті. Функція повертає значення типу double, що є результатом множення по модулю два, яке реалізоване за допомогою операцій зсуву і сумування по модулю два.

Для апробації даної бібліотеки була побудована криптографічна система, в якій реалізований поліноміальний метод шифрування. Тестування криптосистеми підтвердило ефективність і працездатність даної бібліотеки.

Нижче наведено тіло функції AbsMul:

```
publicdoubleAbsMul(doublefirstValue,
doublesecondValue, intsymbolsInAlphabet)
{
doubleresult = 0, rest;
intpow = 0, pow2 = 8, tgenPoly = 137;
if (secondValue>Math.Pow(2, 0))
{
while (Math.Pow(2, pow) <= secondValue)
 {
pow++;
 }
pow--;
 }
if (secondValue != 0)
{
rest = AbsMul(firstValue, (secondValue %
Math.Pow(2, pow)), symbolsInAlphabet);
result = ((int)firstValue<<pow) ^ (int)rest;
while (true)
{
pow2 = 8;
if (result>= Math.Pow(2, 8))
{
while (Math.Pow(2, pow2) <= result)
    {
        pow2++;
    }
pow2--;
result = (int)result ^ ((int)tgenPoly<< (pow2 - 7));
}
else
if (result>symbolsInAlphabet - 1)
{
result = (int)result ^ (int)tgenPoly;break;
}
else
break;
}
```

```
}
else
result = 0;
returnresult;
}
```

Приклад використання функції для реалізації таблиці множення по модулю два розмірністю 127 символів:

```
usingpolynomialMethods;
…
PolyMethodencAlg = newPolyMethod();
…
mtDataGridView.Columns.Clear();
mtDataGridView.Rows.Clear();
for (int i = 0; i < 127; i++)
{
mtDataGridView.Columns.Add("cl"+ i.ToString(),
i.ToString());
mtDataGridView.Rows.Add();
mtDataGridView.Rows[i].HeaderCell.Value
=i.ToString();
}
for (int i = 0; i < 127; i++)
{
for (int j = 0; j < 127; j++)
{
mtDataGridView.Rows[i].Cells[j].Value=encAlg.
AbsMul(i, j, 127);//саме тут відбувається виклик
функції AbsMul, за допомогою якої відбувається
створення таблиці 127 на 127 комірок, що
заповнюються результатами множення по модулю
два вертикального та горизонтального індексу
таблиці.
}}
```

Файл бібліотеки може бути отриманий за електронною адресою sharapov.i.a@gmail.com.

Висновки

Ефективна реалізації операцій над поліномами у вигляді бібліотеки класів забезпечує простоту реалізації методу поліноміального шифрування, який може використовуватись для моделювання апаратно-реалізованих криптосистем.

Список літератури

1. *Ю.Б.Буркатовская, А.Н.Мальчуков, А.Н.Осокин. Быстродействующие алгоритмы деления полиномов в арифметике по модулю два. // Известия Томского политехнического университета. 2006. – Т.309. – № 1, С.19-24.*
2. *У. Питерсон, Э. Уэлдон. «Коды, исправляющие ошибки»: М.: Мир, 1976.*
3. *Темников Ф.Е., Афонин В.А., Дмитриев В.И. Теоретические основы информационной техники. – М.: Энергия, 1971.*
4. *Кавчук А.А. Основы передачи непрерывных сообщений по дискретным каналам связи. Таганрог: ТРТИ, 1978.*
5. *Тутевич В.Н. Телемеханика. – М.: Энергия, 1973.*
6. *Бородин А.Ф. Введение в теорию помехоустойчивого кодирования. М.: Сов. радио, 1968.*
7. *Самойленко С.Н. Помехоустойчивое кодирование. – М.: Наука,1971.*
8. *Удалов А.П., Супрун Б.А. Избыточное кодирование при передаче информации двоичными кодами. М.: Связь,1964.*

Стаття надійшла до редколегії 20.01.2012

Рецензент : д-р техн. наук, проф. С.О.Лук'яненко, Національний технічний університет, Київський політехнічний інститут, Київ.