Торгашова А.В.

ГЕНЕРАЦИЯ НЕПРИВОДИМЫХ МНОГОЧЛЕНОВ

Уральский государственный университет путей сообщения

Генерация неприводимых многочленов является актуальной и сложной на сегодняшний день прикладной задачей, широко используемой и востребованной в криптографических приложениях (генерация открытых и закрытых ключей) и теории кодирования (построение кодов полиномиального кодирования). Генерация неприводимых многочленной есть порождение (нахождение) неприводимых многочленов с заведомо хорошими свойствами, что позволяет использовать их для генерации ключей (закрытых и открытых) в системах защищенного документооборота, например, в системах интернет-банка и клиент-банка.

В работах [4–7] предложены алгоритмы для нахождения многочленов данной степени и порядка при известном многочлене той же степени. Алгоритмы построения многочленов основываются на том, что корни многочленов x и y связаны степенным соотношением, простейшее из них – $y=x^p$. В цитированных выше работах были явно выписаны формулы вычисления коэффициентов для p=3, 5 и 7. Разработана и отлажена программа для перебора многочленов, корни которых связаны соотношением $x \to x^3$. Для произвольного p также могут быть получены аналогичные комбинаторные формулы, эффективные программы и быстрые алгоритмы перехода от корня x к корню x^p. Однако обратный переход сопряжен со значительными вычислительными трудностями. Это может быть использовано для получения односторонних функций, которые могут служить основой построения соответствующих асимметричных криптосистем [6]. При этом можно выписать условия, определяющие возможность генерации всех неприводимых многочленов данной степени. А именно, если степень многочлена – число Мерсенна, а его порядок d – простое число Мерсенна, причём p – первообразный корень по модулю d, то получаем все возможные многочлены при таком переборе. Если же p не является первообразным корнем, то получаем не все многочлены. Достаточным условием полноты перебора является условие того, что степени корня, не вошедшие в перебор, отличаются от вошедших в перебор множителем, равным степени двойки.

Сильной стороной этого метода является последовательность вычисления искомых многочленов, рекуррентность вычисления их коэффициентов через коэффициенты уже найденных многочленов, а также легкость его программной реализации. Данный простой, но эффективный способ генерации элементов ключевого пространства может быть положен в основу надёжных систем криптографической защиты информации. Также преобразование $x \to x^p$ можно использовать для генерации псевдослучайных последовательностей.

Приведем более уточненную формулировку полученных результатов для p=5. Одночлен $a_j a_k a_l a_m a_n$ входит в сумму для коэффициента b_r тогда и только тогда, когда:

- либо когда $j=k=l=m=n=r$, и тогда одночлен имеет вид a_r^5;
- либо когда $l \equiv k \pmod 5$ и $4k+l=5r$, и тогда одночлен имеет вид $a_k^4 a_l$;

− либо когда l, m, и k несравнимы между собой по модулю пять и тогда одночлен имеет вид $a_k^2 a_l^2 a_m$ или $a_k^3 a_l a_m$;

− либо когда все четыре индекса различны и либо l несравним с k, либо m несравним с k, либо n несравним с k и $2k+l+m+n=5r$, и тогда одночлен имеет вид $a_k^2 a_l a_m a_n$;

− либо когда все индексы не равны и несравнимы между собой и тогда одночлен имеет вид $a_j a_k a_l a_m a_n$.

Эти выводы пригодны для программной реализации алгоритма построения неприводимого многочлена $f_5(z)$ по неприводимому многочлену $f(x)$ со степенной связью их корней $z=x^5$. Изложенный метод [4, 6] может быть использован для алгоритмизации построения неприводимого многочлена $f_p(z)$ со связью корней $z=x^p$ при таких p, что p – простое число, по модулю которого двойка является первообразным корнем, так что многочлен неприводим над $GF(2)$, и все его корни есть неединичные корни степени из единицы.

Литература

1. Логарифм Зеха-Якоби в задаче расшифровки / Торгашова А.В., Титов С.С., Баданова О.М., Ициксон М.А. // Проблемы теоретической и прикладной математики. Труды 33-й региональной молодежной конференции – Екатеринбург, 2002.– С.51-55.

2. Яковлев, В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта / Яковлев В.В., Корниенко А.А. // Учебник для вузов ж.-д. транспорта – М.: УМК МПС России, 2002. – 328с.

3. Шнайер, Б. Прикладная криптография. 2-е издание: протоколы, алгоритмы и исходные тексты на языке С+ / Шнайер Б. 1996.

4. Торгашова, А.В. Рекуррентное вычисление коэффициентов степеней экспоненты / Торгашова А.В., Титов С.С., Демкина О.Е. // Проблемы теоретической и прикладной математики. Труды 34-й региональной молодежной конференции. – Екатеринбург, 2003.– С.27-30.

5. Демкина, О.Е. Некоторые задачи полиномиального кодирования / Демкина О.Е. // Безопасность информационного пространства: Материалы региональной конференции. – Екатеринбург: ГОУ ВПО УГТУ – УПИ, 2003. – С.12-13.

6. Торгашова, А.В. Рекуррентное вычисление неприводимых многочленов в задачах двоичного кодирования / Торгашова А.В., Титов С.С., Демкина О.Е. // Молодые ученые – транспорту: Труды IV научно-технической конференции. – Екатеринбург: УрГУПС, 2003. – С. 391-401.

7. Экстремальные задачи полиномиального кодирования / Торгашова А.В., Титов С.С., Моклокова Л.М., Яковлева Е.В., Демкина О.Е., Ициксон М.А. // Проблемы теоретической и прикладной математики. Труды 35-й региональной молодежной конференции. – Екатеринбург: УрО РАН, 2004.– С.46-50.