УДК 004.942

Ю. Е. Бояринова, Т. В. Синькова
Институт проблем регистрации информации НАН Украины
ул. Н. Шпака, 2, 03113 Киев, Украина

Схема разделения секрета с использованием полиномов Лагранжа

Рассмотрена возможность использования гиперкомплексных чисел в качестве коэффициентов полинома Лагранжа.

***Ключевые слова**: задача разделения секрета, полином Лагранжа, фундаментальная теорема Гаусса.*

Введение

Информация имеет важное значение в жизнедеятельности человечества. При этом она становится все более уязвимой из-за возрастающих объемов хранимых и передаваемых данных. Поэтому все большую важность приобретает проблема защиты информации от несанкционированного доступа при передаче и хранении. Сейчас услуги криптографии необходимы почти во всех областях деятельности человека.

Построение систем обработки информации на базе компьютерных сетей приводит к изменению форм обращения информации и появлению необходимости в построении криптографических алгоритмов на основе пороговых схем [1].

Пороговой схемой или схемой разделения секрета называется такая схема, которая позволяет «распределить» секрет между несколькими участниками таким образом, чтобы заранее заданные разрешенные множества участников могли однозначно восстановить секрет, а неразрешенные — не получили никакой дополнительной информации о возможном значении секрета.

Существует некоторая схема разделения, называемая (k,t)-пороговой схемой. В простейшем варианте этой схемы любое сообщение делится на t частей, так что по любым k частям можно восстановить сообщение.

Существуют различные схемы разделения секрета: схема Асмуса–Блума, схема Карнина–Грини–Хеллмана, схема интерполяционных полиномов Лагранжа, разделение секрета с мошенниками, разделение секрета без посторонней помощи, разделение секрета без раскрытия частей, подтверждаемое разделение секрета, схема разделения секрета с мерами предупреждения, разделение секрета с вычеркиванием из списка, векторная схема и др. [2].

Целью работы было рассмотреть возможность использования гиперкомплексных числовых систем в схеме разделения секрета с использованием интерполяционных полиномов Лагранжа.

Общие сведения о схеме разделения секрета с использованием интерполяционных полиномов Лагранжа

Для создания пороговой схемы А. Шамир пользовался полиномиальными уравнениями в конечном поле [3]. Выбираем простое число p, которое больше количества возможных долей и больше самого большого из возможных секретов. Чтобы сделать секрет общим, сгенерируем произвольный многочлен степени $k-1$. Например, если нужно создать $(3,t)$-пороговую схему (для восстановления сообщения C потребуется три доли), генерируется квадратичный многочлен:

$$(ax^2 + bx + C) \bmod p,$$

где p — это случайное простое число, большее любого из коэффициентов.

Коэффициенты a,b выбираются случайным образом, они хранятся в тайне и отбрасываются после распределения долей, C — это сообщение. Простое число должно быть опубликовано.

Доли получаются с помощью вычисления многочлена в n различных точках:

$$r_i = F(x_i).$$

То есть первой долей может быть значение многочлена при $x=1$, второй долей — значение многочлена при $x=2$ и т.д.

Поскольку в квадратных многочленах имеются три неизвестных коэффициента a,b и C, то для создания трех уравнений можно использовать любые три доли. Одной или двух долей будет недостаточно, а четырех или пяти долей будет даже с избытком.

Рассмотрим пример, когда $C=13$. Чтобы создать (3,5)-пороговую схему, в которой любые трое из пяти человек могут восстановить C, сначала получим квадратное уравнение:

$$F(x) = (5x^2 + 9x + 13) \bmod 19.$$

.

Тогда пятью частями являются:

$$r_1 = F(1) = 5 + 9 + 13 (\text{mod} 19) \equiv 8,$$
$$r_2 = F(2) = 20 + 18 + 13 (\text{mod} 19) \equiv 13,$$
$$r_3 = F(3) = 45 + 27 + 13 (\text{mod} 19) \equiv 9,$$
$$r_4 = F(4) = 80 + 36 + 13 (\text{mod} 19) \equiv 15,$$
$$r_5 = F(5) = 125 + 45 + 13 (\text{mod} 19) \equiv 12.$$

Чтобы восстановить сообщение C по трем частям, например r_1, r_3, r_4, решается система линейных сравнений:

$$a \cdot 1^2 + b \cdot 1 + C = 8 (\mathrm{mod} 19),$$

$$a \cdot 3^2 + b \cdot 3 + C = 9 (\mathrm{mod} 19),$$

$$a \cdot 4^2 + b \cdot 4 + C = 15 (\mathrm{mod} 19).$$

Решением будут $a = 5,\ b = 9,\ C = 13$. Таким образом, C восстановлено.

Применение гиперкомплексных чисел в схеме разделения секрета с использованием интерполяционных полиномов Лагранжа

Нам представляется, что данная процедура может быть рассмотрена не только в области вещественных чисел, но и в области комплексных чисел. Основой для этого является то, что как вещественные, так и комплексные числа, с точки зрения математики, являются «полями» [4]. Это приводит к тому, что задача разделения секрета может быть представлена и сформулирована в поле комплексных чисел [5].

Пример 1. Пусть есть многочлен следующего вида:

$$W(X) = ((2e_1 + e_2)X^2 + 3e_2 X + (3e_1 + 2e_2)) (\mathrm{mod}\, 4e_1 + 5e_2).$$

Рассмотрим значение $W(X)$ в пяти точках. Первоначально построим вычеты для модуля $m = m_1 + m_2 = 4e_1 + 5e_2$. Норма этого модуля $N(m) = 41$.

В соответствии с фундаментальной теоремой Гаусса [6] по заданному комплексному модулю $m = m_1 e_1 + m_2 e_2$, норма которого равна $N(m) = {m_1}^2 + {m_2}^2$, и для которого m_1 и q являются взаимно простыми числами, каждое целое комплексное число сравнимо с одним и только одним вычетом из ряда $0,1,2,..., N-1$, строим таблицу вычетов.

Для этого находим коэффициент изоморфного перехода ρ из соотношения:

$$\rho = m_1 u + m_2 v (\mathrm{mod}\, N(m)).$$

Для заданного модуля $m = m_1 + m_2 = 4e_1 + 5e_2$ этот коэффициент $\rho = -9$, позволяет построить таблицу соответствия комплексных и действительных вычетов.

Вещественный вычет	Комплексный вычет	Вещественный вычет	Комплексный вычет
0	0	21	$-2e_1+2e_2$
1	$-4e_1+4e_2$	22	$-e_1+2e_2$
2	$-3e_1+4e_2$	23	$2e_2$
3	$-2e_1+4e_2$	24	e_1+2e_2
4	$-e_1+4e_2$	25	$-3e_1+6e_2$
5	$4e_2$	26	$-2e_1+6e_2$
6	e_1+4e_2	27	$-e_1+6e_2$
7	$2e_1+4e_2$	28	$6e_2$
8	$3e_1+4e_2$	29	e_1+6e_2
9	$-e_1+8e_2$	30	$2e_1+6e_2$
10	$8e_2$	31	$-e_1+e_2$
11	$-3e_1+3e_2$	32	e_2
12	$-2e_1+3e_2$	33	$-4e_1+5e_2$
13	$-e_1+3e_2$	34	$-3e_1+5e_2$
14	$3e_2$	35	$-2e_1+5e_2$
15	e_1+3e_2	36	$-e_1+5e_2$
16	$2e_1+3e_2$	37	$5e_2$
17	$-2e_1+7e_2$	38	e_1+5e_2
18	$-e_1+7e_2$	39	$2e_1+5e_2$
19	$7e_2$	40	$3e_1+5e_2$
20	e_1+7e_2		

Найдем значение многочлена W в точках, соответствующих вычетам в точках 1,2,3,4,5, т.е.:

$$W(X_1)=W(-4e_1+4e_2)=23e_1-74e_2(\bmod 4e_1+5e_2)\equiv -4e_1+5e_2,$$
$$W(X_2)=W(-3e_1+4e_2)=-47e_1+34e_2(\bmod 4e_1+5e_2)\equiv 2e_1+3e_2,$$
$$W(X_3)=W(-2e_1+4e_2)=-17e_1-48e_2(\bmod 4e_1+5e_2)\equiv 4e_2,$$
$$W(X_4)=W(e_1+4e_2)=-47e_1+6e_2(\bmod 4e_1+5e_2)\equiv -e_1+2e_2,$$
$$W(X_5)=W(4e_1)=-29e_1-2e_2(\bmod 4e_1+5e_2)\equiv -2e_1+e_2.$$

Чтобы восстановить сообщение C по трем частям, например W_1,W_2,W_4, решается система линейных сравнений:

$$A\cdot(-4e_1+4e_2)^2+B\cdot(-4e_1+4e_2)+C=-4e_1+5e_2(\bmod 4e_1+5e_2),$$
$$A\cdot(-3e_1+4e_2)^2+B\cdot(-3e_1+4e_2)+C=2e_1+3e_2(\bmod 4e_1+5e_2),$$

$$A \cdot (e_1 + 4e_2)^2 + B \cdot (e_1 + 4e_2) + C = -e_1 + 2e_2 (\mathrm{mod}\, 4e_1 + 5e_2).$$

При решении получаем $C = 3e_1 + 2e_2$.

Пример 2. Пусть есть многочлен следующего вида $K(X) = ((2e_1 + e_2)X^2 + (2e_1 + 3e_2)X + (2e_1 + 5e_2))(\mathrm{mod}\, 5e_1 + 7e_2)$.

Значение нормы $N(5e_1 + 7e_2) = 74$. Выполняя аналогичные вычисления, строим таблицу соответствия комплексных и вещественных вычетов.

Вещественный вычет	Комплексный вычет	Вещественный вычет	Комплексный вычет	Вещественный вычет	Комплексный вычет
0	0	25	$-e_1 + 8e_2$	50	$4e_2$
1	$-6e_1 + 5e_2$	26	$8e_2$	51	$e_1 + 4e_2$
2	$-5e_1 + 5e_2$	27	$e_1 + 8e_2$	52	$2e_1 + 4e_2$
3	$-4e_1 + 5e_2$	28	$2e_1 + 8e_2$	53	$-4e_1 + 9e_2$
4	$-3e_1 + 5e_2$	29	$3e_1 + 8e_2$	54	$-3e_1 + 9e_2$
5	$-2e_1 + 5e_2$	30	$-e_1 + 1e_2$	55	$-2e_1 + 9e_2$
6	$-e_1 + 5e_2$	31	e_2	56	$-e_1 + 9e_2$
7	$5e_2$	32	$-6e_1 + 6e_2$	57	$9e_2$
8	$e_1 + 5e_2$	33	$-5e_1 + 6e_2$	58	$e_1 + 9e_2$
9	$2e_1 + 5e_2$	34	$-4e_1 + 6e_2$	59	$2e_1 + 9e_2$
10	$3e_1 + 5e_2$	35	$-3e_1 + 6e_2$	60	$-2e_1 + 2e_2$
11	$-3e_1 + 10e_2$	36	$-2e_1 + 6e_2$	61	$-e_1 + 2e_2$
12	$-2e_1 + 10e_2$	37	$-e_1 + 6e_2$	62	$2e_2$
13	$-e_1 + 10e_2$	38	$6e_2$	63	$e_1 + 2e_2$
14	$10e_2$	39	$e_1 + 6e_2$	64	$-5e_1 + 7e_2$
15	$-4e_1 + 3e_2$	40	$2e_1 + 6e_2$	65	$-4e_1 + 7e_2$
16	$-3e_1 + 3e_2$	41	$3e_1 + 6e_2$	66	$-3e_1 + 7e_2$
17	$-2e_1 + 3e_2$	42	$4e_1 + 6e_2$	67	$-2e_1 + 7e_2$
18	$-e_1 + 3e_2$	43	$-2e_1 + 11e_2$	68	$-e_1 + 7e_2$
19	$3e_2$	44	$-e_1 + 11e_2$	69	$7e_2$
20	$e_1 + 3e_2$	45	$-5e_1 + 4e_2$	70	$e_1 + 7e_2$
21	$2e_1 + 3e_2$	46	$-4e_1 + 4e_2$	71	$2e_1 + 7e_2$
22	$-4e_1 + 8e_2$	47	$-3e_1 + 4e_2$	72	$3e_1 + 7e_2$
23	$-3e_1 + 8e_2$	48	$-2e_1 + 4e_2$	73	$4e_1 + 7e_2$
24	$-2e_1 + 8e_2$	49	$-e_1 + 4e_2$		

Для дальнейших вычислений возьмем значения: $X_1 = -6e_1 + 5e_2$, $X_2 = -5e_1 + 5e_2$, $X_3 = -4e_1 + 5e_2$, $X_4 = -3e_1 + 5e_2$, $X_5 = -2e_1 + 5e_2$.

Найдем значение многочлена K в этих точках:

$$K(X_1) = K(-6e_1 + 5e_2) = 57e_1 - 97e_2 (\mathrm{mod}\, 5e_1 + 7e_2) \equiv 3e_1 + 5e_2,$$
$$K(X_2) = K(-5e_1 + 5e_2) = 27e_1 - 100e_2 (\mathrm{mod}\, 5e_1 + 7e_2) \equiv -3e_1 + 6e_2,$$
$$K(X_3) = K(-4e_1 + 5e_2) = e_1 - 86e_2 (\mathrm{mod}\, 5e_1 + 7e_2) \equiv 4e_1 + 7e_2,$$
$$K(X_4) = K(-3e_1 + 5e_2) = -21e_1 - 10e_2 (\mathrm{mod}\, 5e_1 + 7e_2) \equiv e_1 + 6e_2,$$
$$K(X_5) = K(-2e_1 + 5e_2) = -35e_1 - 50e_2 (\mathrm{mod}\, 5e_1 + 7e_2) \equiv -2e_1 + 11e_2.$$

Чтобы восстановить сообщение C по трем частям, например K_2, K_3, K_5, решается система линейных сравнений:

$$A \cdot (-5e_1 + 5e_2)^2 + B \cdot (-5e_1 + 5e_2) + C = -3e_1 + 6e_2 (\mathrm{mod}\, 4e_1 + 5e_2),$$
$$A \cdot (-4e_1 + 5e_2)^2 + B \cdot (-4e_1 + 5e_2) + C = 4e_1 + 7e_2 (\mathrm{mod}\, 4e_1 + 5e_2),$$
$$A \cdot (-2e_1 + 5e_2)^2 + B \cdot (-2e_1 + 5e_2) + C = -2e_1 + 11e_2 (\mathrm{mod}\, 4e_1 + 5e_2).$$

При решении получаем $C = 2e_1 + 5e_2$.

Выводы

Таким образом, схема разделения секрета с использованием полинома Лагранжа также может быть построена с гиперкомплексными числами. В статье был рассмотрен пример построения этой схемы с использованием комплексных чисел. Благодаря развитию фундаментальной теоремы Гаусса на другие гиперкомплексные числовые системы, можно надеяться получить положительные результаты при расширении комплексных чисел в такой схеме разделения секрета.

1. *Ященко В.В.* Введение в криптографию / Ященко В.В. — М.: МЦНМО, 2001. — 288 с.

2. *Шнайер Б.* Прикладная криптографія / Шнайер Б. –М.: Триумф, 1995. — 816 с.

3. *Shamir A.* How to Share a Secret / Shamir A. // Communications of the ACM. —1979, Nov. — Vol. 24, N. 11. — P. 612–613.

4. *Акушский И.Я.* Машинная арифметика в остаточных классах / Акушский И.Я., Юдицкий Д.И. — М.: Сов. Радио, 1968. — 440 с.

5. *Синьков М.В.* Развитие задачи разделения секрета / Синьков М.В., Бояринова Ю.Е., Калиновский Я.А., Трубников П.В. // Реєстрація, зберігання і оброб. даних. — 2003. — Т. 5, № 4. — С. 90–96.

6. *Синьков М.В.* Непозиционные представления в многомерных числовых системах / Синьков М.В., Губарени Н.М. — К.: Наук. думка, 1979. — 140 с.

Поступила в редакцию 27.02.2009