Ю.Е. Бояринова, Т.В. Синькова (ИПРИ НАН Украины, Киев)

Прикладные математические направления и задача разделения секрета

Нами показано, что теоретико-числовые свойства системы сравнений и расширение поля комплексных чисел на коммутативные и некоммутативные гиперкомплексные числовые системы (ГЧС) более высоких порядков является основой для существенного повышения стойкости криптографической задачи разделения секрета.

В своей постановке задача разделения секрета опирается на решение системы линейных сравнений по совокупности взаимно простых модулей $m_1 ... m_n$. Произведение этих модулей M должно быть таким, что оно характеризует верхнюю границу числового диапазона, внутри которого может располагаться секрет. Определенную трудность составляет решение обратной задачи – восстановление секрета из остаточных представлений по совокупности модулей. При решении криптографической задачи разделения секрета используется китайская теорема об остатках

$$x = \sum_{i=1}^{n} \alpha_i M_i N_i (mod M), \tag{1}$$

где α_i - остаточное представление секрета x по соответствующему модулю m_i, $i = 1...n$, $(m_j, m_k) = 1$, $M = \prod_{i=1}^{n} m_i$, $M_i = \prod_{k \neq i} m_k$, $N_i M_i \equiv 1 (mod\ m_i)$.

В (1) на предпоследнем шаге решается сравнение по модулю M, что теоретически правильно, но на практике недопустимо. Разработан метод решения обратной задачи таким путем, что в процессе вычислений ни одна величина не выходит за пределы диапазона $0 - M$.

Также при решении этой задачи возникает трудность нахождения обратной по модулю величины N_i в (1). Это связано с тем, что в гиперкомплексных числах нет аналога функции Эйлера. В этом случае применяем фундаментальную теорему Гаусса об изоморфизме [1]. Формулируется она так: по заданному комплексному модулю $A = a_1 e_1 + a_2 e_2$, норма которого равна $N(A) = a_1^2 + a_2^2$ и для которого a_1 и a_2 являются взаимно простыми числами, каждое целое комплексное число сравнимо с одним и только одним вычетом из ряда $0, 1, 2, ..., N - 1$. Это позволяет найти обратную величину N_i в вещественных вычетах, затем перейти обратно в область ГЧС и все вычисления далее выполняются в ГЧС. То есть в любом конкретном случае для выбранной ГЧС нужно доказывать аналог фундаментальной теоремы Гаусса, что представляется единственным путем устранения трудностей нахождения обратной величины при отсутствии функции Эйлера. В [2] были доказаны аналоги фундаментальной теоремы Гаусса для некоторых ГЧС.

Нами было доказано, что применение ГЧС в задаче разделения секрета дает повышение стойкости в зависимости от длины ключа порядка $2^{78} - 2^{156}$.

Работа выполнена при поддержке Государственного фонда фундаментальных исследований Украины; проект № Ф29.1/026.

[1] Виноградов И.М. Основы теории чисел. – М. 1952. –148с.

[2] Синьков М.В., Губарени Н.М. Непозиционные представления в многомерных числовых системах. – Киев: Наукова думка, 1979. –140с.
