Анализ одной схемы цифровой подписи

М.М. Глухов

В работе [1] предлагается криптографическая схема электронной цифровой подписи (ЭЦП), основанная на сложности проблемы извлечения корня большой простой степени в абелевых группах. В качестве групп предлагается использовать мультипликативные группы определенных трехмерных ассоциативных и коммутативных алгебр над кольцом Z/p^2 вычетов целых чисел по модулю p^2, где p – большое простое число.

В [1] рассмотрены два алгоритма извлечения корня p-й степени из элементов выбранной авторами группы Γ, и показано, что сложность наименее трудоемкого из них равна $O(p\sqrt{p})$ операциям умножения элементов группы Γ. В связи с этим утверждается, что эти группы являются перспективными для решения задачи синтеза алгоритмов ЭЦП.

В данной работе в общем виде описано строение группы Γ и на этой основе доказано следующее утверждение.

Теорема. *Алгоритм вычисления корня p-й степени из элемента ξ группы Γ имеет сложность $O(1)$ двоичных операций, если $Ord\,\xi < p^2$, и $O(\log^3 p)$ двоичных операций, если $Ord\,\xi \geq p^2$.*

Литература

1. Щербаков В.А., Костина А.А., Молдовяну П.А., Молдовян Н.А. Примитивы цифровой подписи: конечные группы с трехмерной цикличностью. Вопросы защиты информации, № 3, С.-Петербург, 2009, 9-15.
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. Изд-во «Лань», Санкт-Петербург-Москва-Краснодар, 2011.